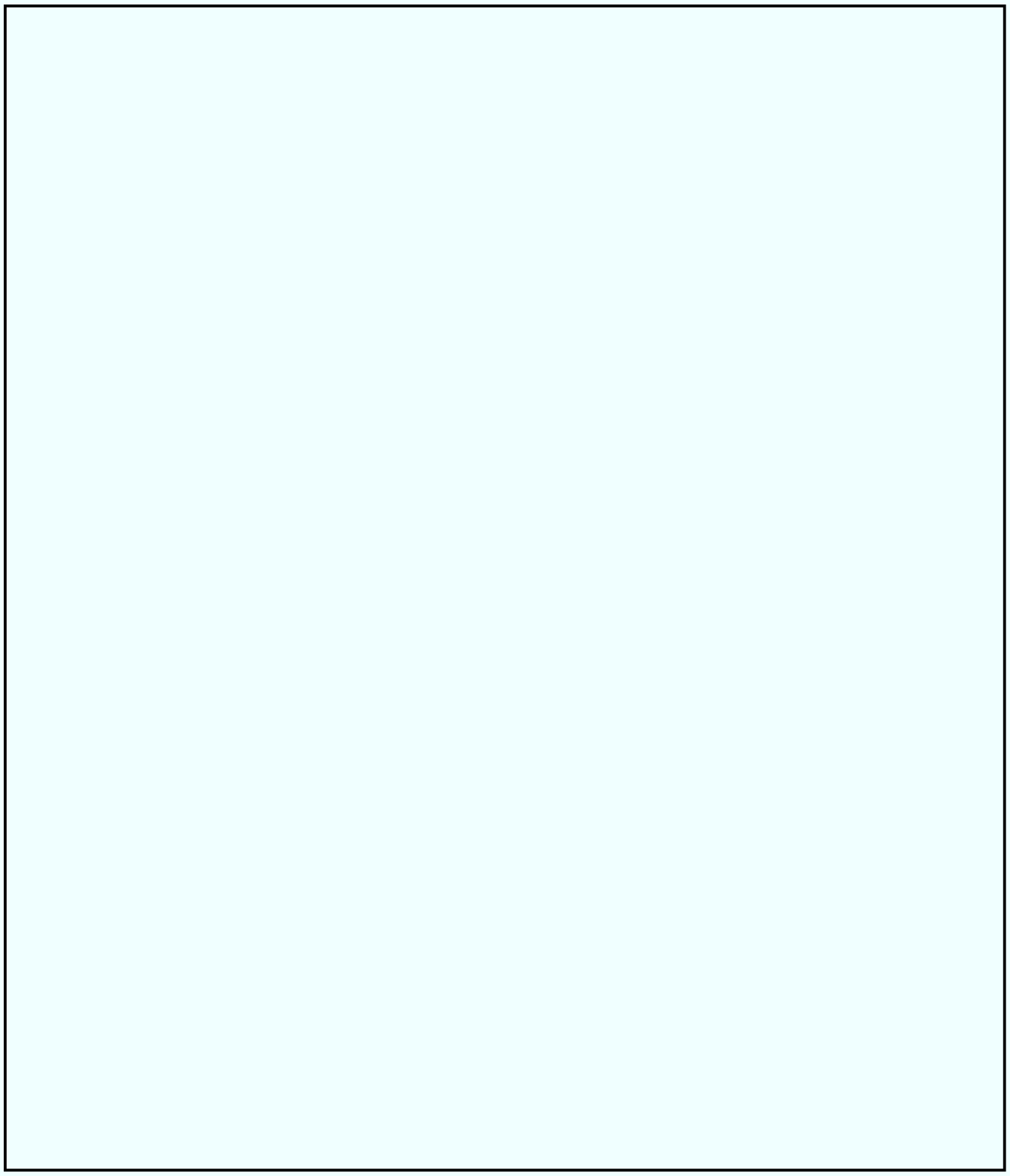
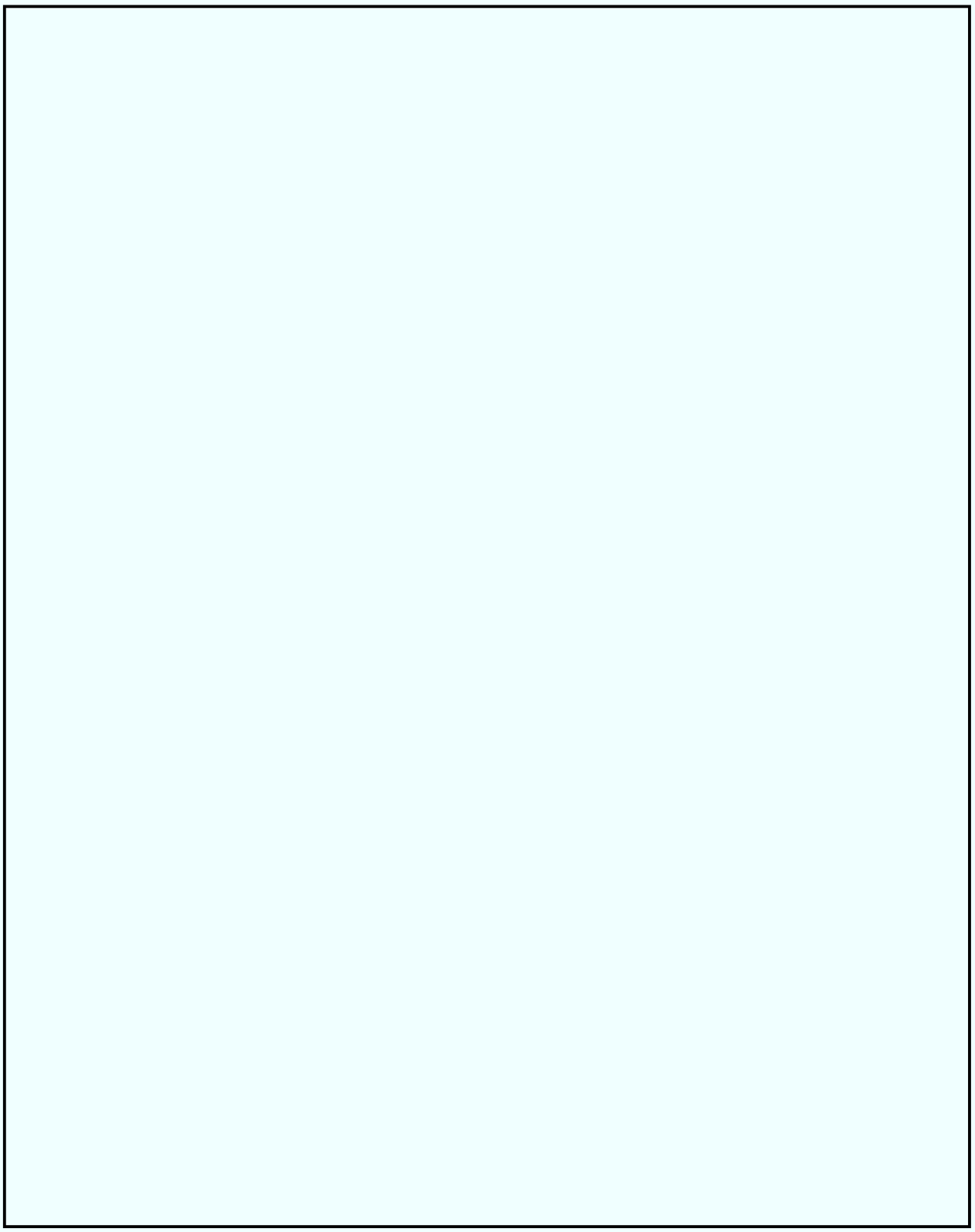
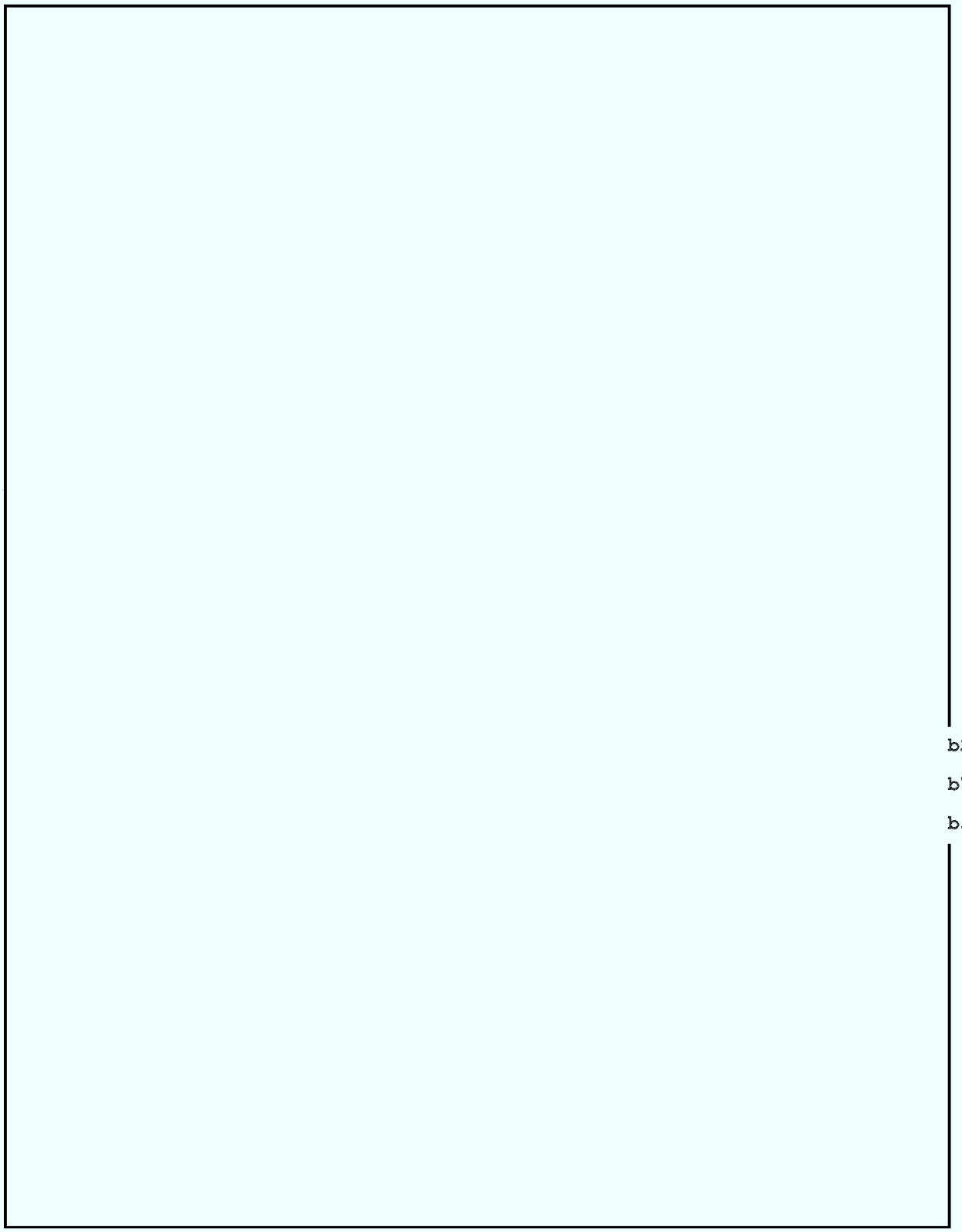


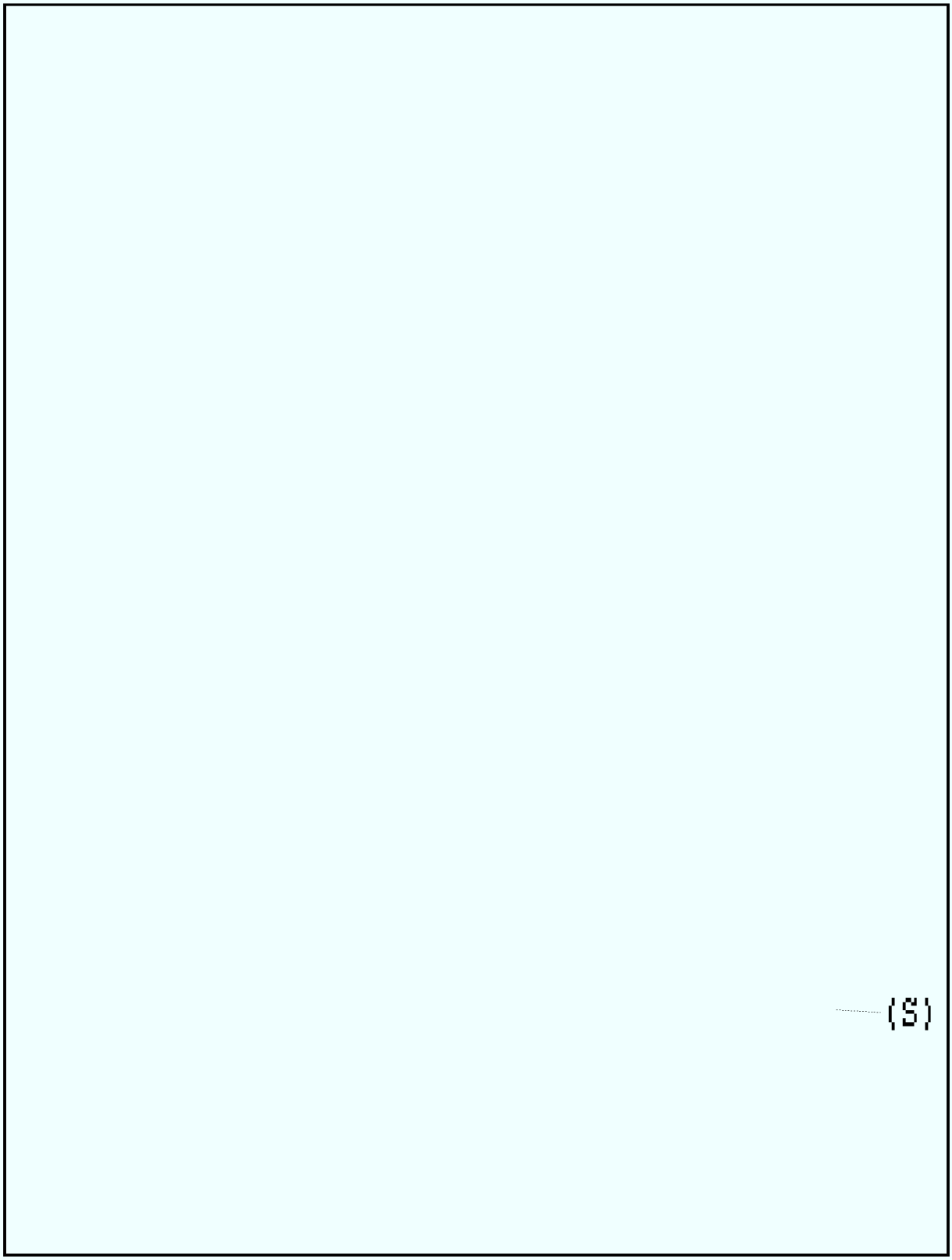
b6
b7C
b5



b5

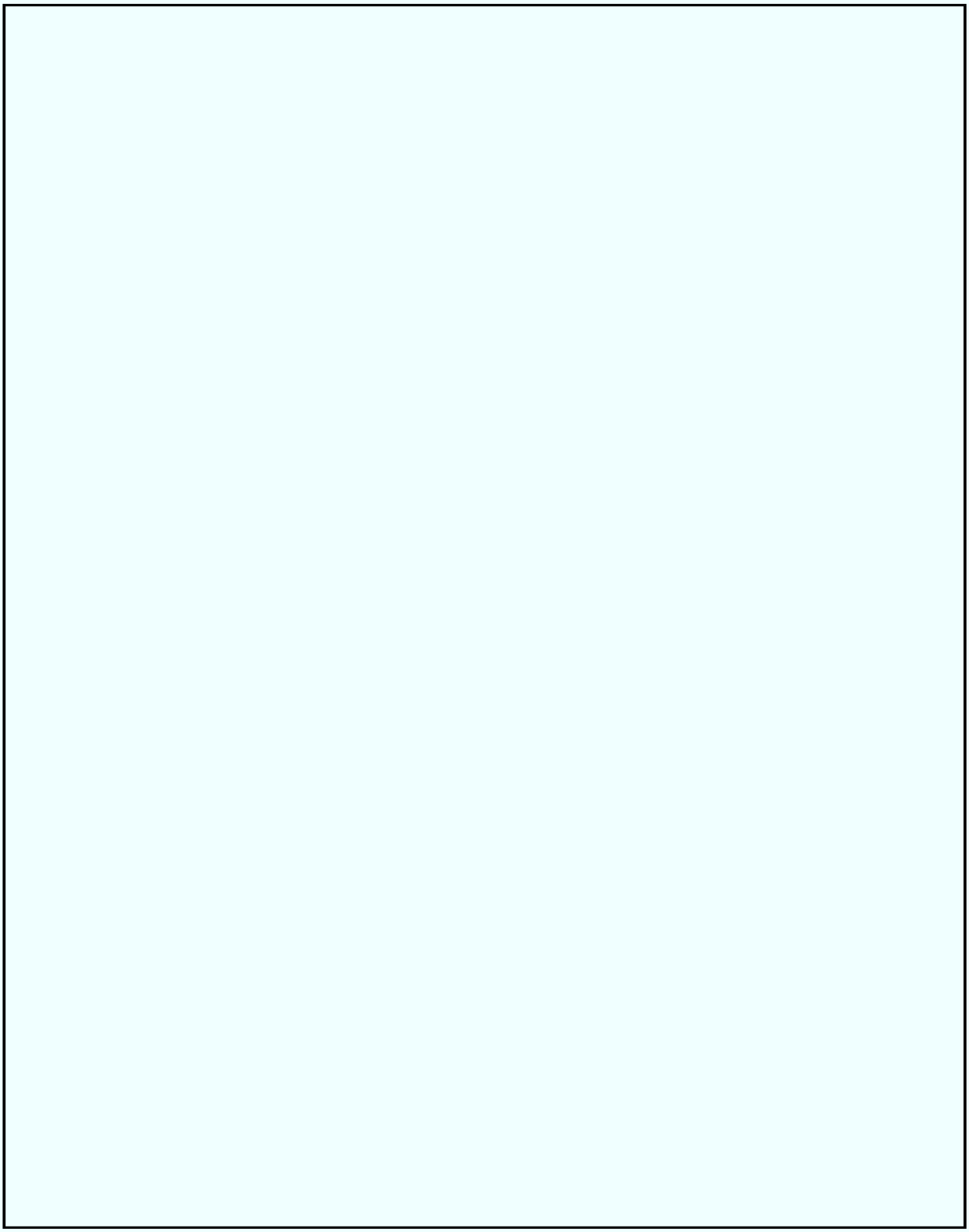


b2
b7E
b5

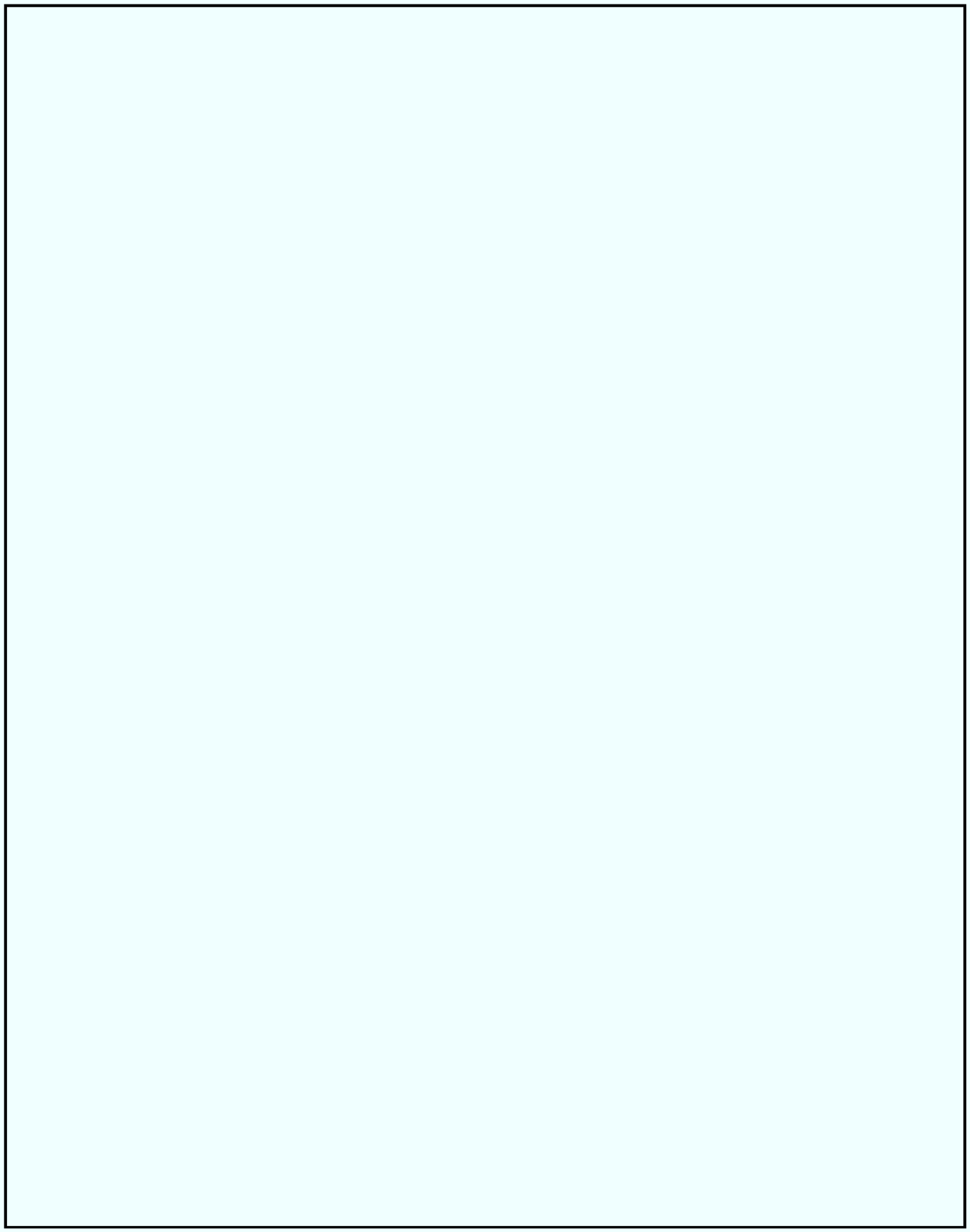


b1
b2
b7E
b5

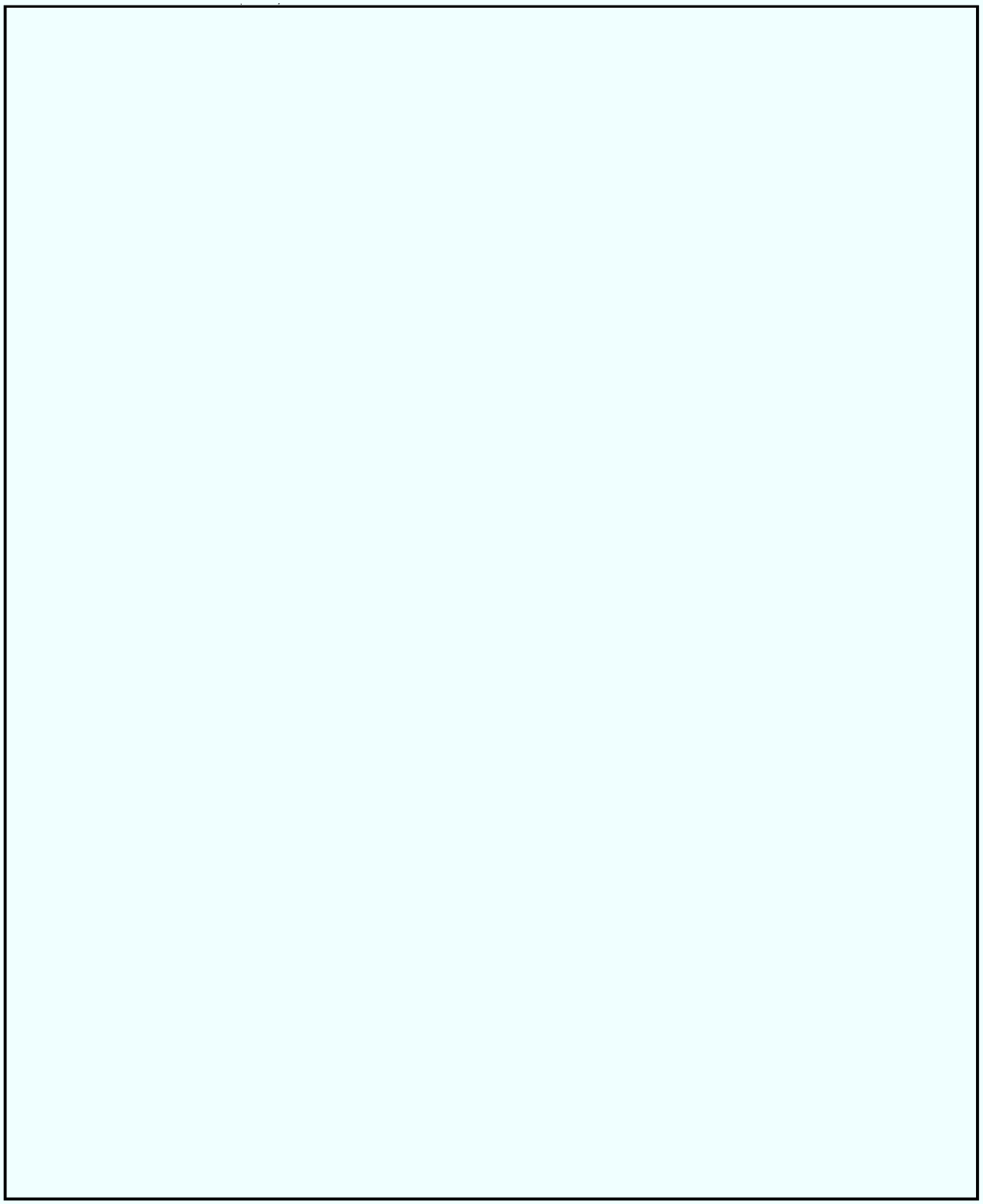
(S)



b5



b5



b5

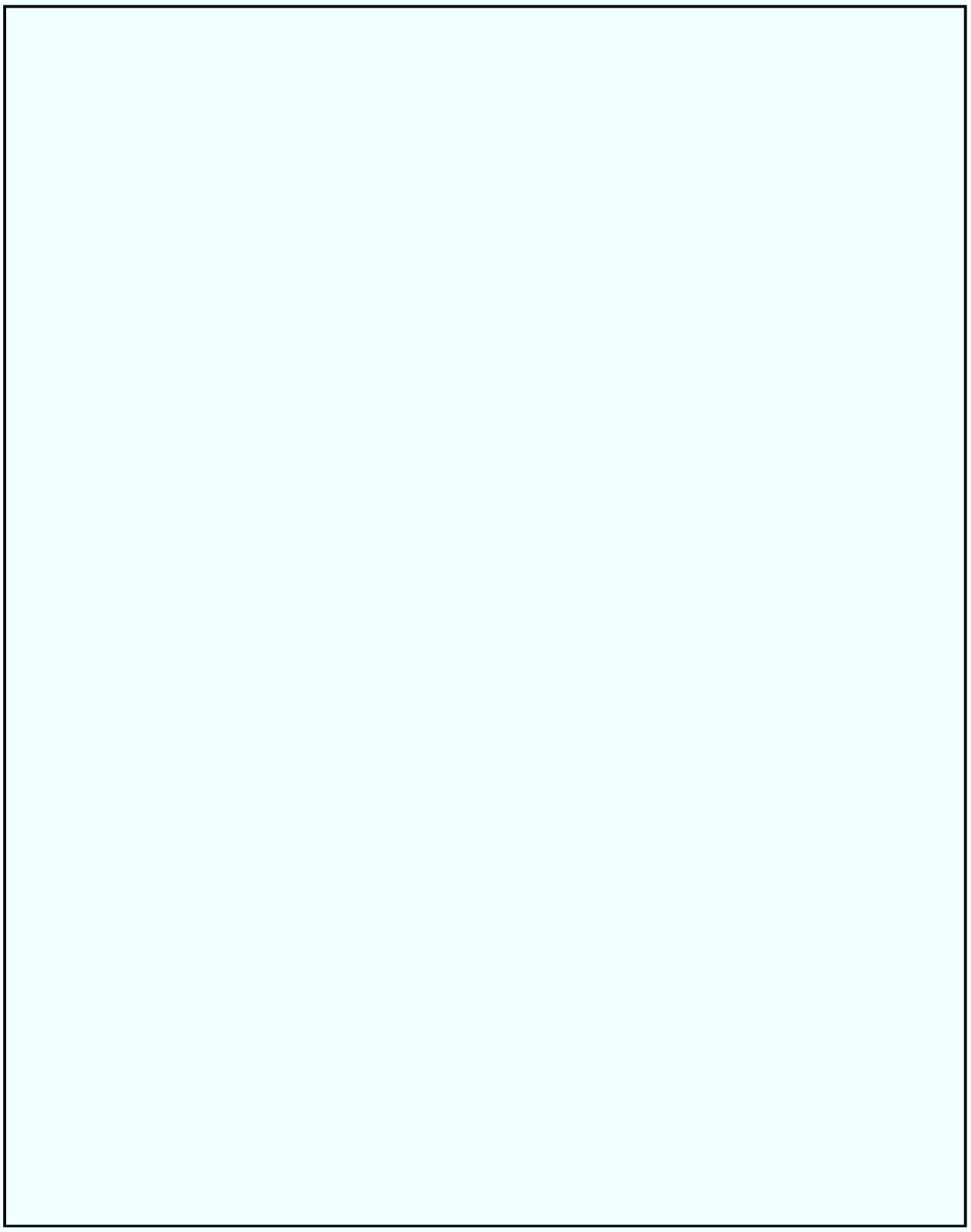
~~SECRET~~

DATE: 11-18-2005
CLASSIFIED BY 65179DMH/lr2 Ca#-05-CV-0845-
REASON: 1.4 (C)
DECLASSIFY ON: 11-18-2030

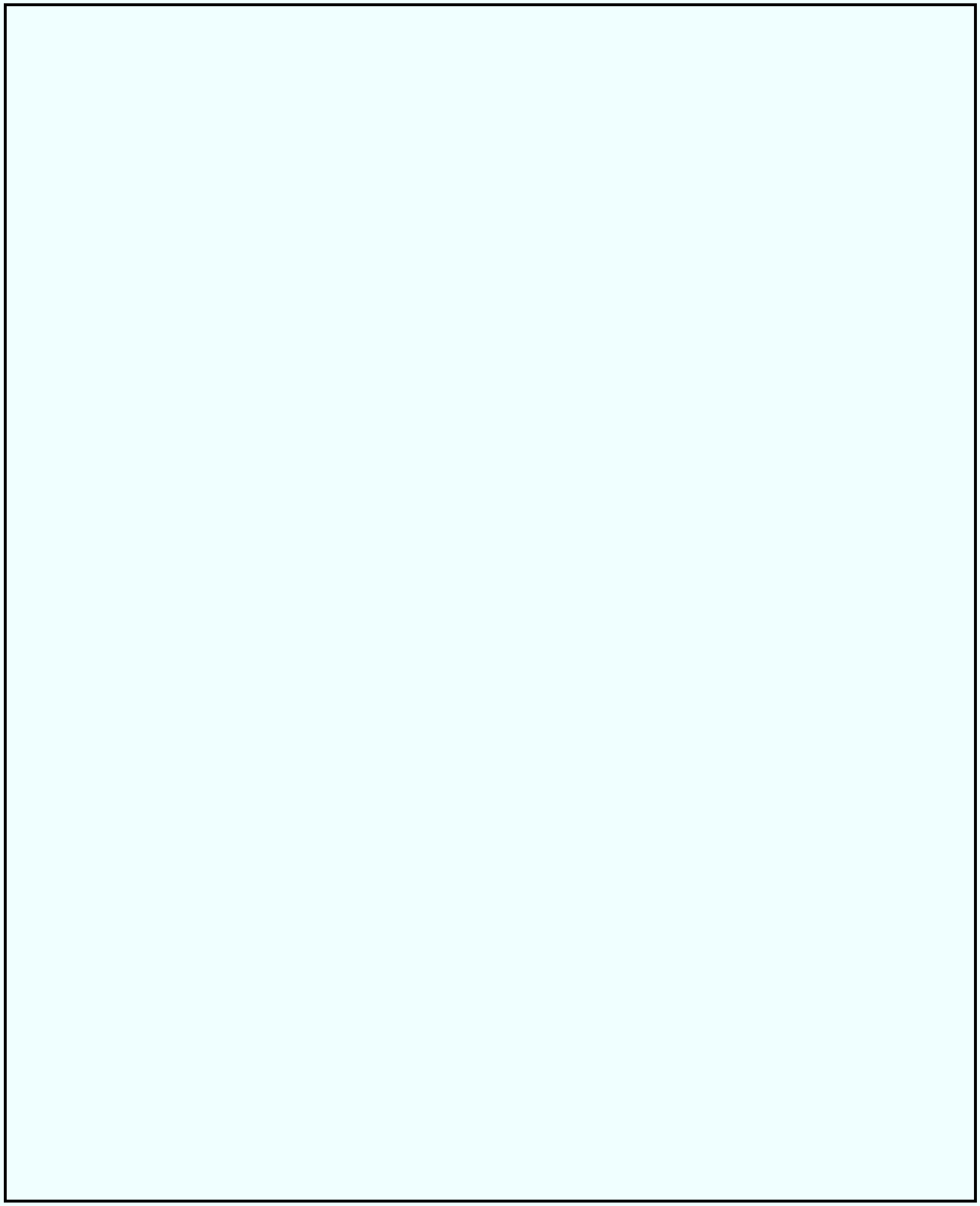
ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

b5

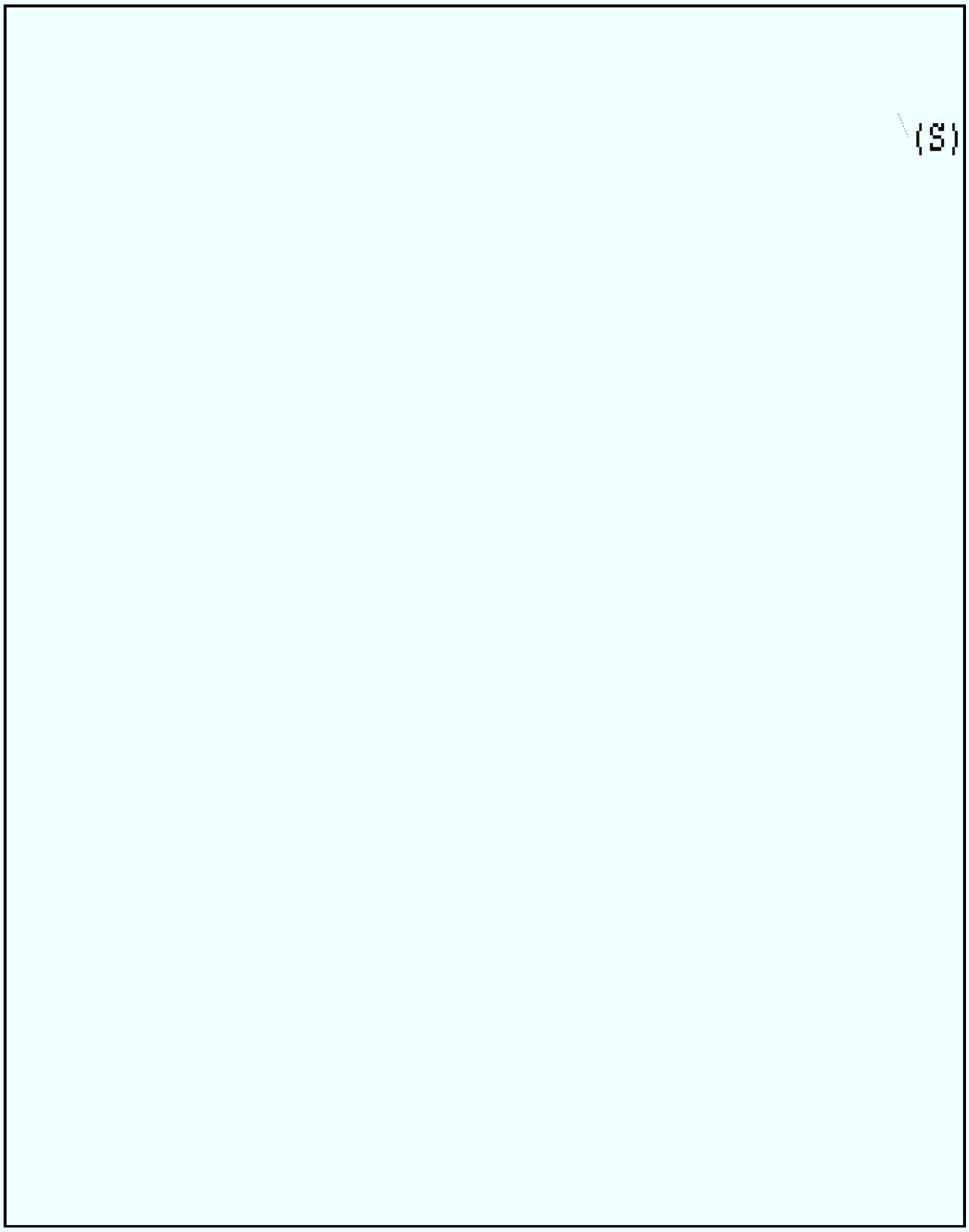
~~SECRET~~



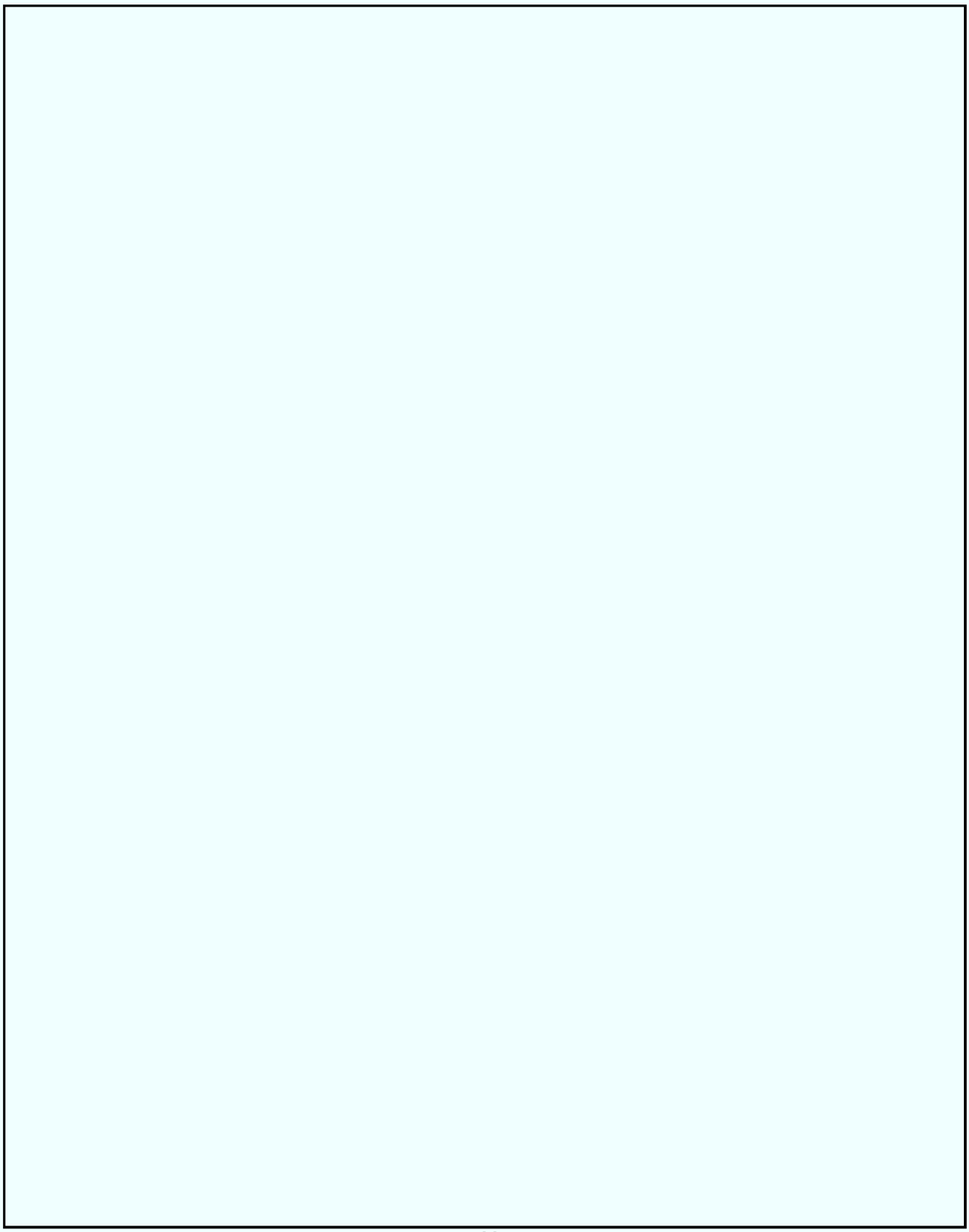
b5
b2
b7E



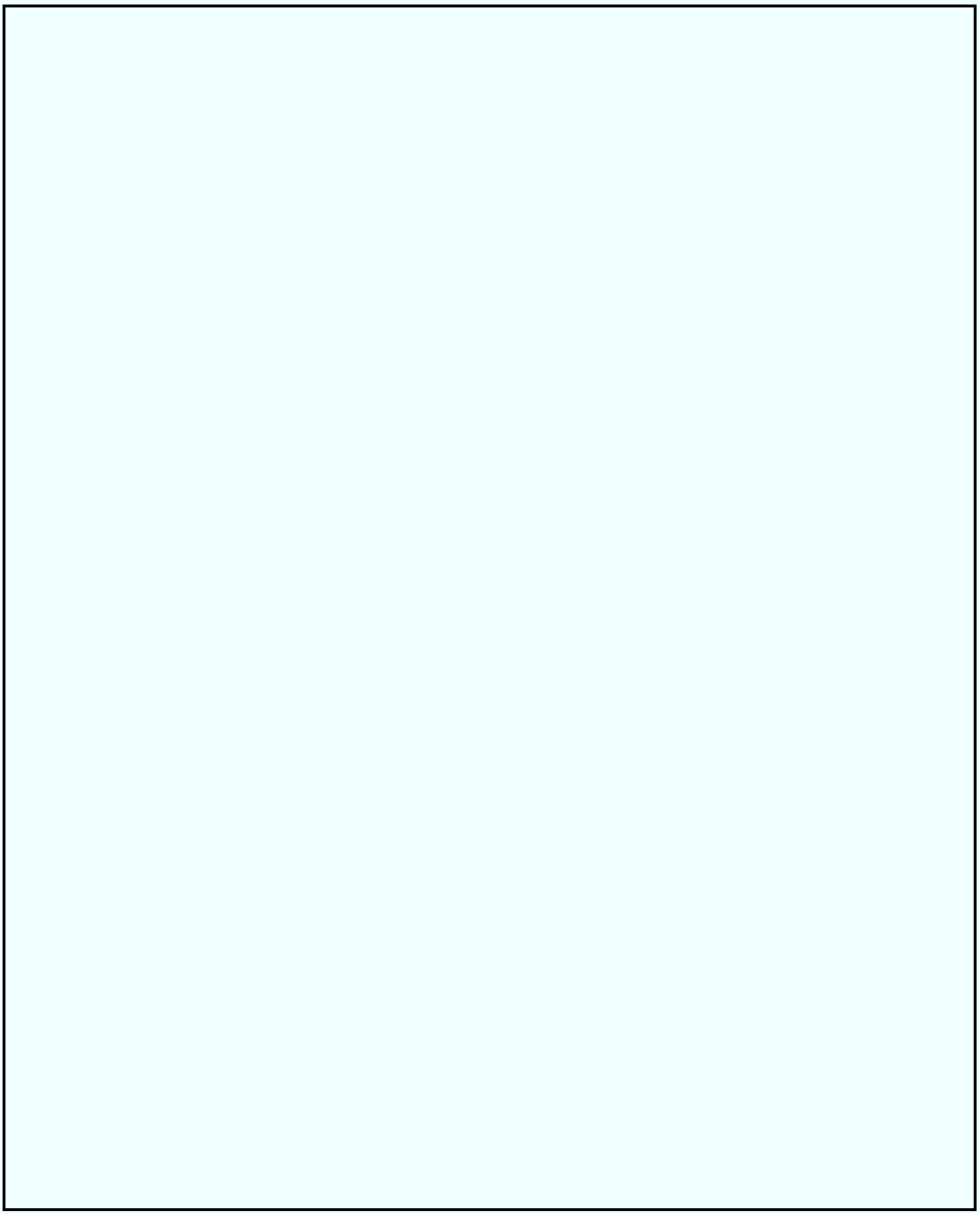
b5
b7E



b5
b2
b7E
b1



b5



b5
b2
b7E

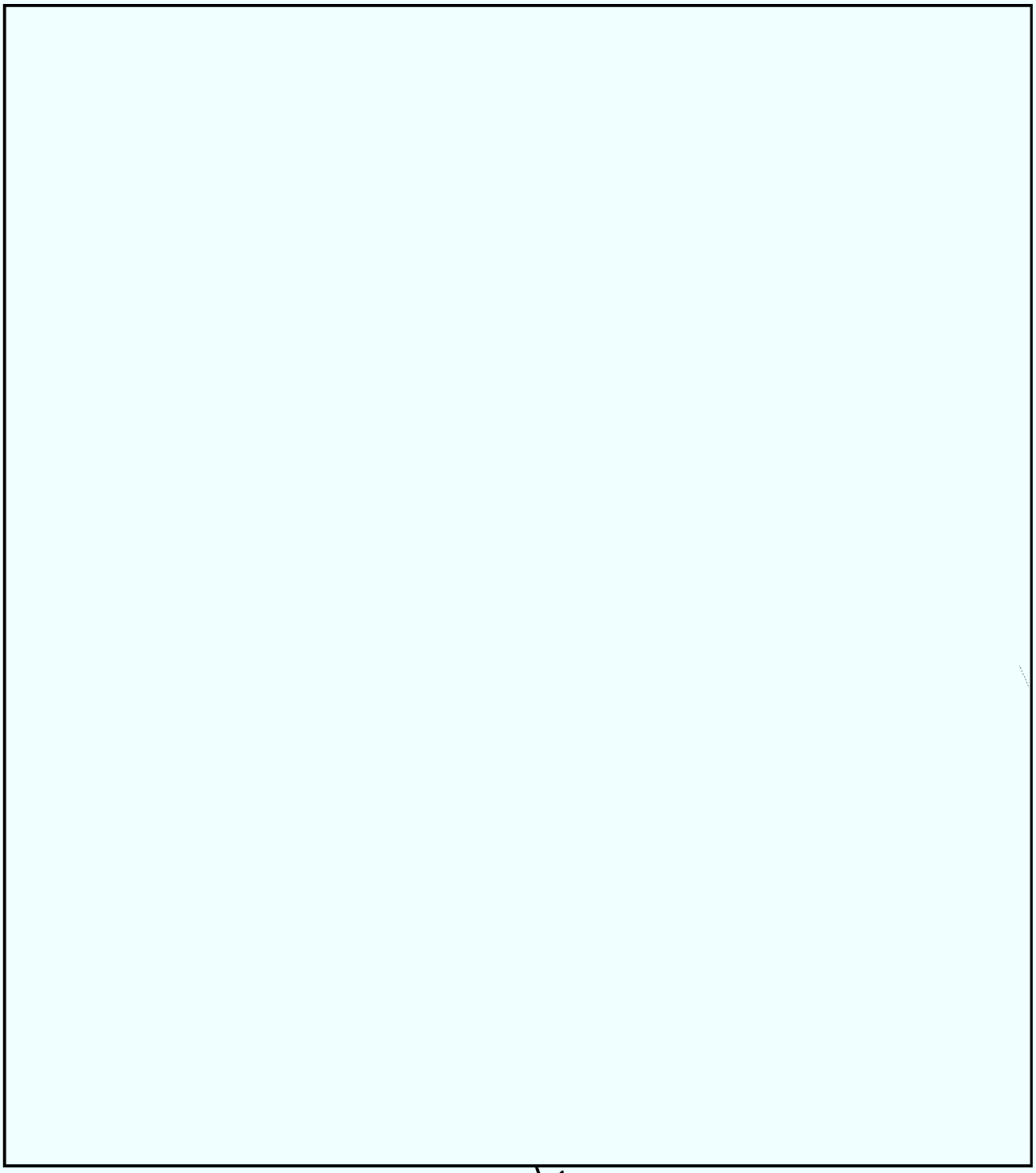
FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 62
Page 44 ~ Duplicate
Page 45 ~ Duplicate
Page 46 ~ Duplicate
Page 47 ~ Duplicate
Page 48 ~ Duplicate
Page 49 ~ Duplicate
Page 50 ~ Duplicate
Page 51 ~ Duplicate
Page 52 ~ Duplicate
Page 53 ~ Duplicate
Page 54 ~ Duplicate
Page 55 ~ Duplicate
Page 56 ~ Duplicate
Page 57 ~ Duplicate
Page 58 ~ Duplicate
Page 59 ~ Duplicate
Page 60 ~ Duplicate
Page 61 ~ Duplicate
Page 62 ~ Duplicate
Page 63 ~ Duplicate
Page 64 ~ Duplicate
Page 65 ~ Duplicate
Page 66 ~ Duplicate
Page 67 ~ Duplicate
Page 68 ~ Duplicate
Page 69 ~ Duplicate
Page 70 ~ Duplicate
Page 71 ~ Duplicate
Page 72 ~ Duplicate
Page 73 ~ Duplicate
Page 74 ~ Duplicate
Page 75 ~ Duplicate
Page 76 ~ Duplicate
Page 77 ~ Duplicate
Page 78 ~ Duplicate
Page 79 ~ Duplicate
Page 80 ~ Duplicate
Page 81 ~ Duplicate
Page 82 ~ Duplicate
Page 83 ~ Duplicate
Page 84 ~ Duplicate
Page 85 ~ Duplicate
Page 86 ~ Duplicate
Page 87 ~ Duplicate

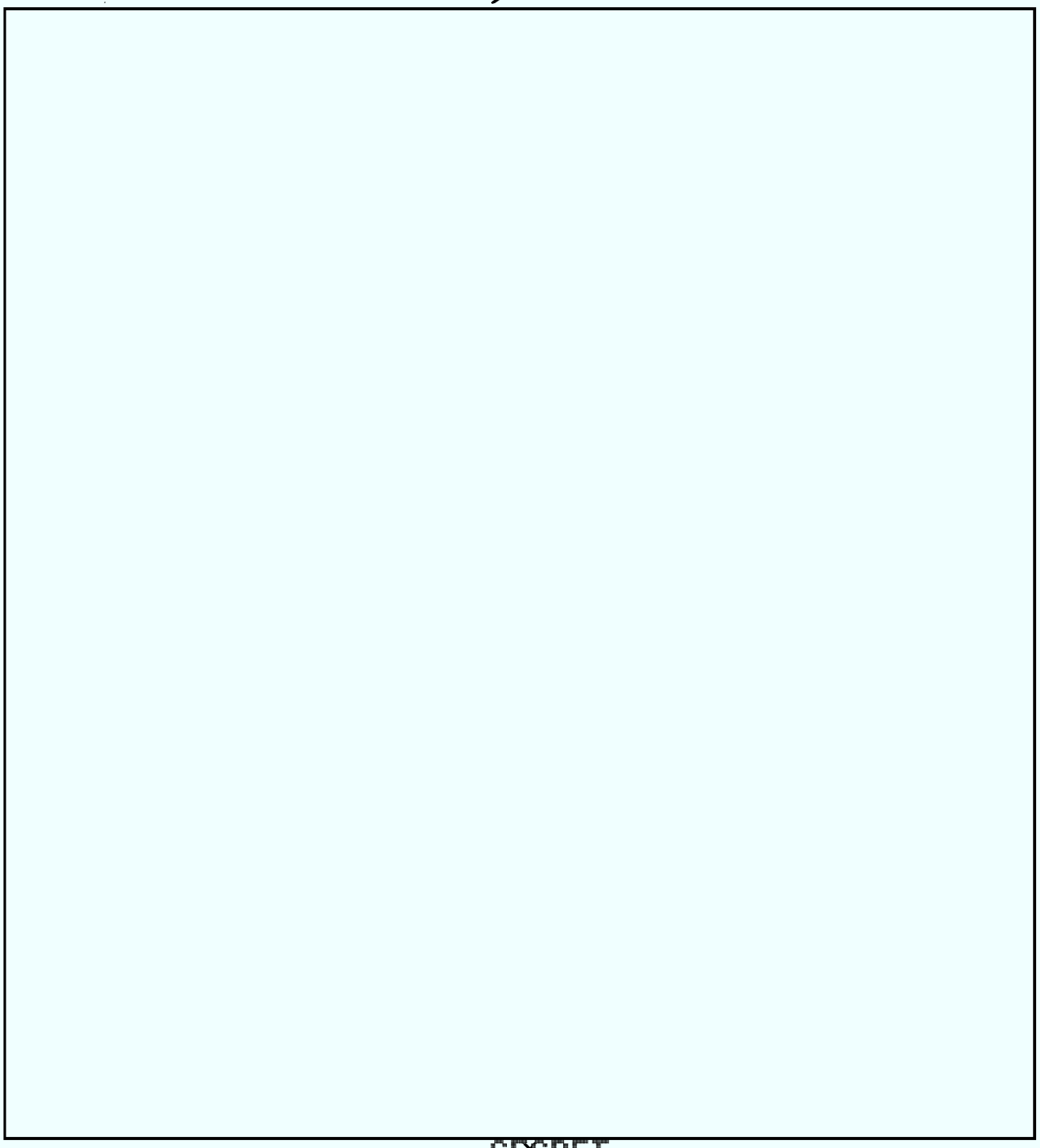
Page 88 ~ Duplicate
Page 89 ~ Duplicate
Page 90 ~ Duplicate
Page 91 ~ Duplicate
Page 92 ~ Duplicate
Page 93 ~ Duplicate
Page 94 ~ Duplicate
Page 95 ~ Duplicate
Page 96 ~ Duplicate
Page 97 ~ Duplicate
Page 98 ~ Duplicate
Page 99 ~ Duplicate
Page 100 ~ Duplicate
Page 101 ~ Duplicate
Page 102 ~ Duplicate
Page 103 ~ Duplicate
Page 104 ~ Duplicate
Page 105 ~ Duplicate

b5

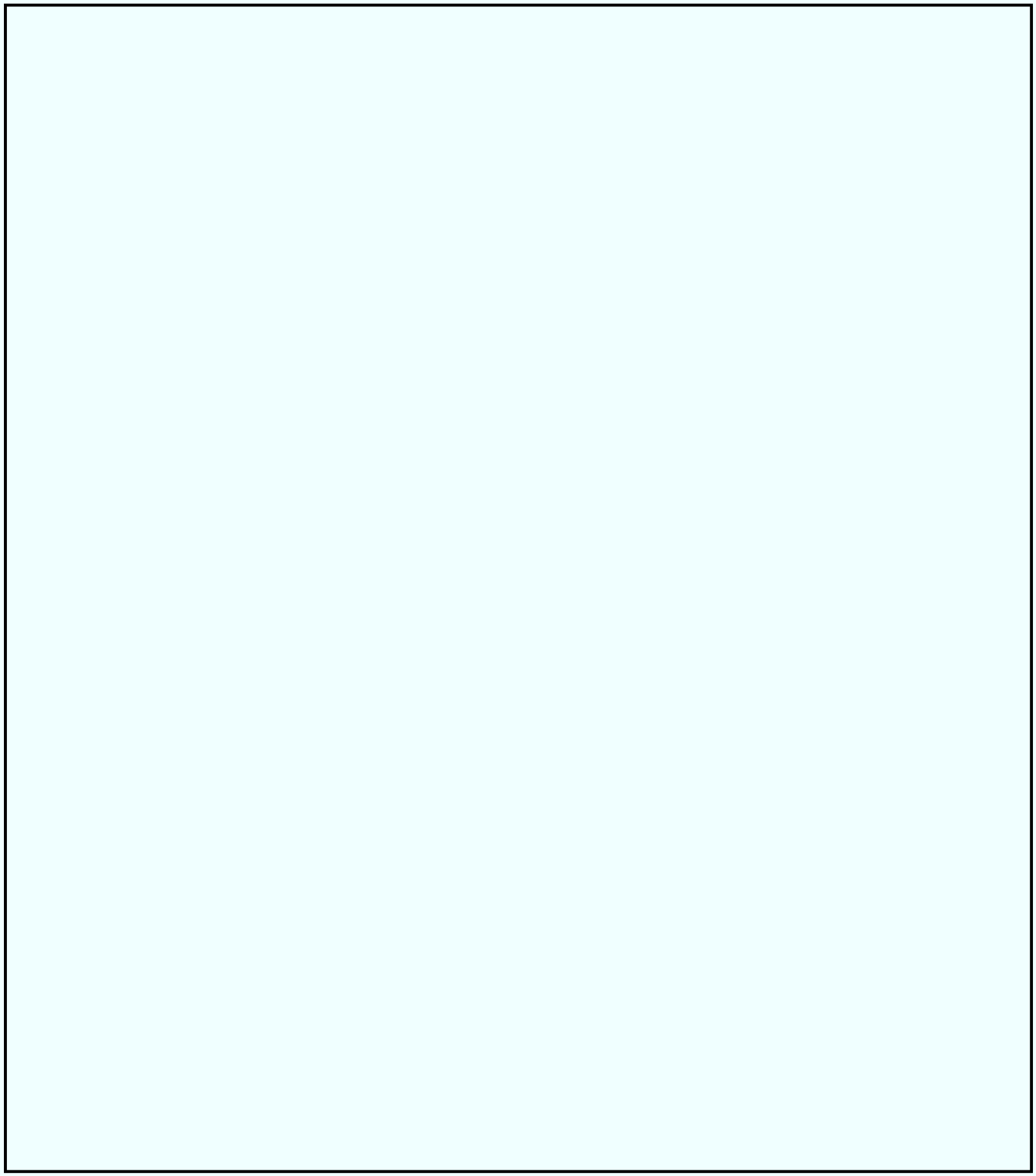


b1
b2
b5

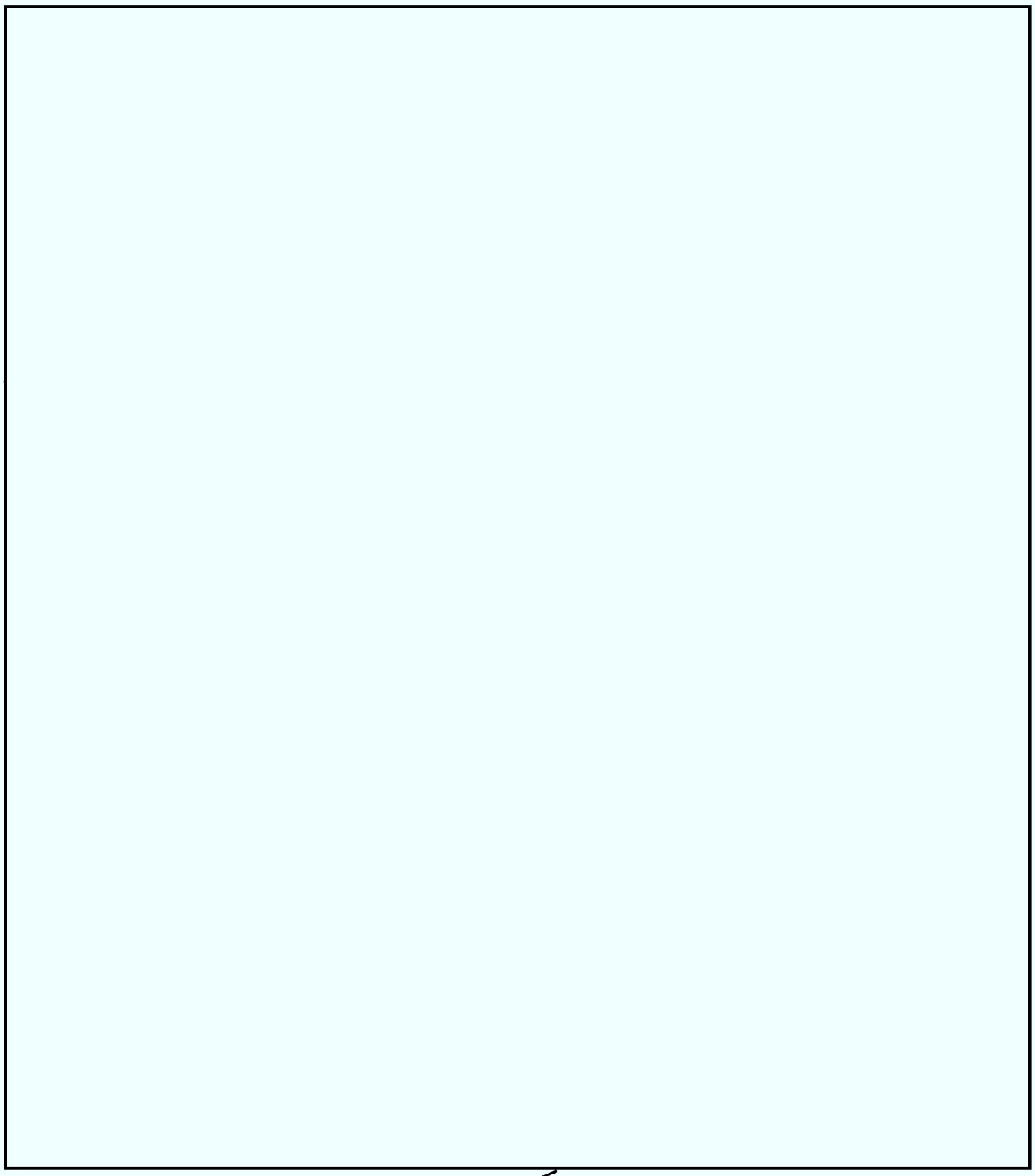
(S)



b5



b5



b5

~~SECRET~~

Responses of Robert S. Mueller, III
Director
Federal Bureau of Investigation
Based Upon July 23, 2003 Testimony
Before the Senate Committee on the Judiciary

Classification per OGA letter dated 08-17-2005

Questions Posed by Senator Hatch

As you know, I have been - and remain - concerned about the issues surrounding the death of Kenneth Michael Trentadue, an inmate who died in the Federal Transfer Center (FTC), in Oklahoma City, Oklahoma, on August 21, 1995. At approximately 3 a.m. on August 21, 1995, FTC correctional officers found Mr. Trentadue hanging by a bed sheet around his neck from a grate in his cell.

FTC officials notified the Oklahoma City FBI about Trentadue's death. I understand that a number of entities, including the FBI, the Justice Department's Civil Rights Division, the Justice Department's Inspector General's Office, the Oklahoma Medical Examiner's Office and the Oklahoma County District Attorney's Office have investigated this matter and reached a determination that Mr. Trentadue was not murdered but committed suicide. Notwithstanding the results of these investigations, I continue to have concerns as to the circumstances of Mr. Trentadue's death. To this end, I want to ask several follow up questions relating to the death of Kenneth Michael Trentadue:

1. **Please describe the FBI's involvement in the investigation of Mr. Trentadue's death, and the steps taken by the FBI during its investigation. In describing the FBI's involvement, please address all aspects of the FBI's investigation, including witness interviews, collection and processing of evidence, and all forensic examinations.**

Response:

The FBI's Oklahoma City Division was notified of Mr. Trentadue's death on August 21, 1995. The Oklahoma City Division took photographs, collected evidence, and opened an investigation into Mr. Trentadue's death. During the first few months of the investigation, the Oklahoma City Division interviewed Bureau of Prisons personnel at the Federal Transfer Facility, sent investigative leads to other field offices requesting that they locate and interview Trentadue family members and inmates who had been at the Federal Transfer Facility at the time of Mr. Trentadue's death, and sent evidence to the FBI Laboratory for forensic examination. In December 1995, the Oklahoma City Division assigned an additional Agent to the investigation in order to increase the investigative effort, and after that time additional forensic tests and numerous interviews were conducted.

Leahy 33. Finding 16 of the Joint Inquiry Report states that prior to September 11, 2001, "there was no coordinated U.S. Government-wide strategy to track terrorist funding and close down their financial support networks." Please describe the current strategy being used to track terrorist funding. What has been done since September 11th to "close down" financial support networks of terrorist activities? If the PATRIOT Act was used in any measure to "close down" a financial support network, please describe those efforts and results in detail.

Response:

Currently, there exists a much better understanding of terrorist financing methods than prior to the 9/11 attacks. More sophisticated and effective processes and mechanisms to address and target terrorist financing continue to be developed and to evolve. Pro-active approaches are increasingly being used. Awareness throughout the world on the part of law enforcement, government agencies, regulators, policy makers, and the private sector of terrorist financing methods, suspicious financial activity, and vulnerabilities is much higher since 9/11. International cooperation has reached unparalleled levels. Outreach with, and cooperation from, the private sector has been outstanding and continues to develop, particularly the level of two-way interaction between law enforcement and the private sector. The ability to access and obtain this type of information immediately has significantly enhanced the FBI's ability to identify, investigate, and resolve immediate threat situations involving potential terrorist activity. For example, the ability to monitor specifically identified financial activity has been invaluable not only to investigations ongoing in the United States, but also to foreign law enforcement and intelligence agencies in related investigations.

Extensive training and support of international investigations by the FBI's Terrorist Financing Operations Section (TFOS) has led to Agent visits, exchanges, and training programs involving a variety of countries in Europe, Southeast Asia, the Middle East, and South America. In support of specific high-profile joint terrorist financial investigations, a number of countries and agencies, including the United Kingdom, Switzerland, Canada, and Europol, have detailed investigators to TFOS on a temporary duty basis. TFOS has engaged in extensive coordination with authorities of numerous foreign governments in terrorist financing matters, leading to joint investigative efforts throughout the world. These joint investigations have successfully targeted the financing of several overseas al Qaeda cells, including those located in Indonesia, Malaysia, Singapore, Spain, and Italy. Furthermore, with the assistance of relationships established with the central banks of several strategic countries, successful disruptions of al Qaeda financing have been accomplished in countries such as the United Arab Emirates, Pakistan, Afghanistan, and Indonesia.

TFOS has developed a specific curriculum regarding terrorist financing/money laundering crimes for use in international training. This curriculum includes such topics as: acquiring and handling evidence in document intensive financial investigations, major case management techniques,

forensic examination tools, and methods of terrorist financing. At the request of DOS, TFOS has led an interagency team to provide this curriculum to a number of countries identified as needing law enforcement training on conducting terrorist financing investigations (training in approximately 38 countries is currently scheduled).

TFOS has cultivated and maintains contact with private industry and government sources/persons who can provide financial data, including real-time monitoring of financial transactions. Many of these contacts can be reached or accessed regarding emergencies 24 hours a day 7 days a week, allowing TFOS to respond rapidly to critical incidents.

Through these contacts, TFOS has access to data and information from a variety of entities including: banking institutions; credit/debit card services; money services businesses; securities and brokerage firms; insurance companies; travel agents; Internet service providers; the telecommunications industry; law enforcement agencies; federal and state regulatory agencies; public and open source data providers; the intelligence community; and international law enforcement and intelligence contacts. The timeliness and accessibility of the data are contingent on a variety of factors including whether the acquisition of the information requires legal process, the search capabilities of the data provider, and the size and depth of the data request. The ability to access and obtain this type of information quickly has significantly enhanced the FBI's ability to identify, investigate, and resolve immediate threat situations involving potential terrorist activity.

The ability to identify and track financial transactions and links after a terrorist act has occurred, or terrorist activity has been identified, represents only a small portion of the mission; the key lies in exploiting financial information to identify previously unknown terrorist cells, recognize potential terrorist activity/planning, and predict and prevent potential terrorist acts. Prior to 9/11, less emphasis was placed on addressing the mechanisms and systems associated with terrorist financing and disrupting them before they could be utilized to further terrorist activities. Since 9/11, TFOS, together with DOJ's Criminal Division's Counterterrorism Section, has begun a number of proactive link analysis initiatives to identify potential terrorists and terrorist related financing activities.

The overriding goal of these projects is to proactively identify potential terrorists and terrorist related individuals, entities, mechanisms, and schemes through the digital exploitation of data. To accomplish this, TFOS seeks to: 1) identify potential electronic data sources within domestic and foreign government and private industry providers; 2) create pathways and protocols to acquire and analyze the data; and 3) provide both reactive and proactive operational, predictive, and educational support to investigators and prosecutors.

Information sharing is critical to all of our efforts. The intelligence community, including the FBI, produces and obtains tremendous amounts of classified intelligence information. While much of the information can be of significant value in terrorist finance investigations, the value will not be realized or maximized absent the ability to filter the information, analyze it, and

disseminate it in an appropriate manner to those who can make the best use of the information. Toward this end, TFOS participates, among other joint activities, in joint endeavors involving the CIA, FBI, Treasury Department, DOJ, and DHS involving potential terrorist-related financial transactions. TFOS has personnel detailed to the CIA Counterterrorism Cente[redacted] (S) b1

The NSC formalized the PCC at the end of 2001. The Department of Treasury chairs the PCC and representatives from the CIA, DOD, DOJ, DHS, NSC, DOS, and FBI attend meetings. The PCC generally meets at least once a month to coordinate the United States government's campaign against terrorist financing. The meeting generally focuses on ensuring that all relevant components of the federal government are acting in a coordinated and effective manner to combat terrorist financing.

Our efforts to combat terrorism have been greatly aided by the authorities of the USA PATRIOT Act. Success in preventing another catastrophic attack on the United States homeland would have been much more difficult, if not impossible, without the Act. It has already proved extraordinarily beneficial in the war on terrorism, and our opportunities to use it will only increase. Most importantly, the PATRIOT Act has produced greater collection and sharing of information within the law enforcement and intelligence communities.

Title III of the Act, known as the International Money Laundering Anti-Terrorist Financing Act of 2001, has armed us with a number of new weapons in our efforts to identify and track the financial structure supporting terrorist groups. Past terrorist financing methods have included the use of informal systems for transferring value in a manner that is difficult to detect and trace. The effectiveness of such methods should be significantly eroded by the Act, which establishes stricter rules for correspondent bank accounts, requires securities brokers and dealers to file Suspicious Activity Reports (SARs), and mandates that certain money services register with FinCEN and file SARs for a wider range of financial transactions.

Other provisions of the Act have considerably aided our efforts to address the terrorist threat including: strengthening the existing ban on providing material support to terrorists and terrorist organizations; the authority to seize terrorist assets; and the ability to seize money subject to forfeiture in a foreign bank account by authorizing seizure of a foreign bank's funds held in a United States correspondent account.

Leahy 34. **In your July 22, 2003 response to questions posed by Senator Cantwell following our June 6, 2002 hearing, regarding concerns that new authorities under the PATRIOT Act will be abused by the FBI (Question 6), you stated, "The FBI has a number of internal and external safeguards in place today that did not exist in the past." You then cited as "two key external safeguards" Executive Order 12333 - which was signed by President Reagan in 1981 -- and the FCIG - which was put in place by Attorney General Reno**

in 1995. You also cited as an "important internal safeguard" the Intelligence Oversight Board established by Executive Order 12863 - which President Clinton issued in 1993.

A. On what basis did you state that these "internal and external safeguards" are "in place today" but "did not exist in the past?"

Response:

The safeguards referenced in the question, Executive Order 12333 and the FCIG, were cited in response to a question that asked, "What assurances can you give us that these new authorities will not be abused in the name of terrorism or intelligence matters, as similar authorities had been abused by the FBI in the past?" We believed that the question's mention of "past abuses" referred to the sort of activities exposed in the 1976 report of the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, better known as the "Church Committee." Executive Order 12333 and the FCIG did not exist during that era, but are in place now. We did not mean to suggest that these safeguards were not in existence when the USA PATRIOT Act was passed.

B. Can you identify any safeguards against FBI abuse of its PATRIOT Act and other investigative authorities that are now in place, but did not exist prior to September 11, 2001?

Response:

There are formal and informal safeguards against FBI abuse of its investigative authorities that did not exist prior to September 11, 2001. First, some of the investigative authorities that were created or expanded by the USA PATRIOT Act contain safeguards against abuse. For example, Section 214 of the Act altered the standards for obtaining a pen register under FISA. Such a pen register may be obtained upon a certification that the information likely to be obtained is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities. Section 214 also now requires that the pen register applicant certify to the court that the underlying investigation of a United States person is not conducted solely on the basis of activities protected by the First Amendment. Such a certification requirement ensures that individuals will not be investigated solely because of what they say or how they worship. Section 214 also preserved the existing court-order requirement. Now, as before, law enforcement cannot install a pen register unless it applies for and receives permission from the FISA court.

Likewise, Section 216 (which codified the applicability of the criminal pen register/trap and trace investigative authority to Internet communications) contains a number of safeguards and restrictions. Section 216 preserved all of the law's pre-existing standards. As before, law enforcement officials must obtain court approval before installing a pen register and must show

that the information sought is relevant to an ongoing investigation. The pen/trap statute (18 U.S.C. chapter 206) was amended throughout to make clear that the contents of communications may not be the intended object of a pen register or trap and trace order. Also, in response to concerns about the FBI's investigative tool DCS1000 (formerly known as Carnivore), the USA PATRIOT Act imposed stringent reporting requirements on the government's installation of government-owned pen/trap devices on public providers' packet-switched data networks. (See 18 U.S.C. section 3123(a)(3).)

In addition, since the USA PATRIOT Act was passed, FBI agents have received guidance concerning appropriate implementation of certain provisions of the Act. This guidance will serve as a safeguard against FBI abuse of its PATRIOT Act and other investigative authorities. For example, Section 203 of the Act permitted law enforcement to share with the intelligence community information obtained from grand juries and Title III wiretaps. Pursuant to the Act, on September 23, 2002, the Attorney General issued Guidelines for Disclosure of Grand Jury and Electronic, Wire, and Oral Interception Information Identifying United States Persons. These Guidelines require labeling of information that identifies United States persons so that it will be properly retained and disseminated by intelligence agencies.

Congressional oversight of the FBI's activities also provides some assurance that the FBI is conducting investigations in accordance with the Constitution and other law. Some of the investigative authorities modified by the USA PATRIOT Act contain safeguards in the form of requirements to report to Congress on use of these new authorities. For example, Section 215 of the Act amended the statute granting access to business records for foreign intelligence and international terrorism investigations, codified at 50 U.S.C. section 501. Pursuant to 50 U.S.C. section 502, on a semiannual basis, the Attorney General must fully inform the IC concerning all requests for production and must also provide the Committees on the Judiciary a report on the numbers of requests and orders.

In at least one instance, a law passed after the USA PATRIOT Act created an additional safeguard by imposing an additional reporting requirement. The Electronic Communications Privacy Act, codified beginning at 18 U.S.C. section 2701, provides privacy protection for electronic communications, such as e-mail and associated records. It also outlines the compulsory process that law enforcement can use to obtain both the content of communications and records held by an electronic communications service provider or a remote computing service, most often an Internet Service Provider. The USA PATRIOT Act created a voluntary disclosure provision that explicitly permits, but does not require, a service provider to disclose customer records to law enforcement in emergencies involving an immediate risk of death or serious physical injury to any person. 18 U.S.C. section 2702(b)(7); 18 U.S.C. section 2702(c)(4). With the passage of the Homeland Security Act of 2002, P.L.107-296, section 225(d)(2), the FBI was required to provide information on emergency disclosures received. This information must also be reported to Congress one year after enactment of the Homeland Security Act of 2002.

From: [redacted] FBI)
To: [redacted] FBI], [redacted]
Date: Mon, Apr 12, 2004 1:38 PM
Subject: Search and arrest of [redacted] on [redacted]

b6
b7C
b6
b7A
b7C

UNCLASSIFIED
NON-RECORD

On [redacted] at approx. 7:30 a.m., we executed a search warrant for the residence of [redacted]

[redacted]

b6
b7A
b7C

[redacted]

b7A

An arrest warrant for [redacted] was prepared based upon [redacted]

[redacted]

b6
b7A
b7C

[redacted] father [redacted] came to the residence at about 8:15 a.m. and had his attorney, [redacted] represented [redacted] was allowed to leave the scene with his father later in the morning. [redacted] father and attorney voluntarily brought [redacted] to the District Court for the 2:30 p.m. initial appearance on [redacted] The arrest warrant was issued for [redacted]

[redacted]

b6
b7A
b7C

[redacted] was taken to the FDC in [redacted] and will be held there until his detention hearing on [redacted] at 3:00 p.m.

The search went off without a hitch and everyone did a remarkable job working as a team and helping out. SA [redacted] did an excellent job as [redacted] and SSA [redacted] did an excellent job overseeing the search. At the end of the day, approximately 75 pieces of evidence were seized, of which 70 were transported by bureau plane to the East Coast and have been take to the lab in Edgewood, Maryland. [redacted] Aunt [redacted] who lives in the house next door to the apartment over her garage where [redacted] was living, was very complementary for how courteous we were in handling the matter. [redacted] Fire Department Battalion [redacted] who assisted during the entire operation, was also complementary and told me, "what you did today was a public service to our community."

b6
b7A
b7C

UNCLASSIFIED

CC: [redacted] [FBI], [redacted]

b7C
b6

b6
b7C

[redacted] (DO) (FBI)

From: [redacted] LA) (FBI)
Sent: Thursday, September 23, 2004 2:19 PM
To: LA MAIL All Employees
Subject: Agents only: Patriot Act Reporting Requirements

UNCLASSIFIED
RECORD 197A-LA-C233355

All FBI field offices are required to track the use of the Patriot Act provisions. Many provisions of the act will expire in 2005 unless renewed by Congress. Thus, we are tracking our use of the provisions. Please reply to this email if you have used any of the provisions identified below between 07/01/04 and the present. Please provide the number of times it was effectively used and specific information regarding why the technique was helpful.

Provisions that will expire on 12/31/2005:

1. Voicemail stored by a communication provider (§§ 2510 and 2703);
2. Nationwide search warrants for email (§ 220);
3. Information sharing (between criminal and CI) (§ 203);
4. Voluntary disclosure by ISP in emergencies (§ 212);
5. Immunity from civil liability for those person giving the FBI information in compliance with a FISA order (§ 225);
6. New T-III predicate crimes (chemical weapons, terrorism, and computer fraud/abuse);
7. Roving FISA surveillance (§ 206);
8. New standard for FISA pen/trap - relevancy (§ 214);
9. New standard for business records (§ 215);
10. New primary purpose for FISA - where FISA is only "a significant purpose" (§ 218); and
11. Monitoring communications of computer trespassers with victim consent (§ 217).

UNCLASSIFIED

U.S. House of Representatives
Committee on the Judiciary
F. James Sensenbrenner, Jr., Chairman

---

http://www.house.gov/judiciary
News Advisory
May 20, 2003
For immediate release

Contact:
Jeff Lungren/Terry Shawn - 202-225-2492
Dena Graziano 202-226-6888

Sensenbrenner/Conyers Release Justice Department Oversight Answers Regarding USA PATRIOT Act and War on Terrorism

WASHINGTON, D.C. – House Judiciary Committee Chairman F. James Sensenbrenner, Jr. (R-Wis.) and Ranking Member John Conyers, Jr. (D-Mich.) today released the answers (**http://www.house.gov/judiciary/patriotlet051303.pdf**) received last week from the Justice Department regarding the USA PATRIOT Act and the war on terrorism. Chairman Sensenbrenner and Rep. Conyers wrote Attorney General John Ashcroft on April 1, 2003 (**http://www.house.gov/judiciary/patriot040103.htm**) requesting information on these issues.

Chairman Sensenbrenner said, "The Justice Department should be commended for the timing and thoroughness of these answers. These answers will assist the Judiciary Committee in fulfilling its legislative and oversight responsibilities and should prove helpful in any future debate about extending all or part of the USA PATRIOT Act. In addition, I hope Members and the public will review the Department's answers for an accurate understanding of what the USA PATRIOT Act authorizes, and how this law is being implemented."

Ranking Member Conyers said, "I appreciate the fact that the Justice Department responded to our queries in a timely basis. I wish they would have been more forth coming in terms of manner in which and how freely the new powers have been used. I look forward to engaging in further oversight with the Department on this critical civil liberties issue."

This Justice Department stated the following in its response:

> ~Congress did not authorize a new innovation with section 215 (production of tangible records including books, records, papers, documents, etc.). Grand juries investigating ordinary crimes traditionally have the power to issue subpoenas to all manner of businesses, including libraries and bookstores. For example, federal grand juries subpoenaed records from numerous libraries during the Unabomber investigation.
>
> ~Section 215 of the USA PATRIOT Act imposes more restrictions on its use than a federal grand jury subpoena for the same records. First, a court must explicitly authorize the use of section 215 to obtain business records. Second, section 215 contains explicit safeguards for activities protected by the First Amendment, unlike federal grand jury subpoenas. Third, section 215 requires, for an investigation relating to a U.S. person, that the information be sought in an investigation to protect against international terrorism or clandestine intelligence activities.

~There has been no challenge to the propriety or legality of National Security Letters.

~There have been no administrative disciplinary proceedings or civil actions initiated under section 223 of the Act for unauthorized disclosures of intercepts.

~The Department of Justice has requested a judicial order delaying notice of the execution of a warrant under section 213 forty-seven times, and the courts have granted every request.

~ government has asked a court to find reasonable necessity for a seizure in connection with delayed notification under this section fifteen times, and the courts have granted fourteen of the requests.

~The court once has rejected the government's argument that a seizure was reasonably necessary. The court authorized the warrant but did not authorize seizure because it believed that photographs of relevant items in the storage unit would be sufficient.

~The most common period of a delay of notification of a warrant authorized by courts is seven days. Courts have authorized specific delays of notification as short as one day and as long as ninety days; other courts have permitted delays of unspecified duration lasting until the indictment was unsealed.

~The government has sought an extension of the period of delayed notice 248 times. This number includes multiple extensions for a single warrant.

~A court has never rejected the government's request for delayed notification on the ground that the period for giving delayed notice was unreasonable.

~The Department cites the recent indictment of Sami Al-Arian and other alleged members of a Palestinian Islamic Jihad (PIJ) cell in Tampa, Florida, as a case that benefitted from the Act's new standard of "a significant purpose" rather than "the purpose." The USA-PATRIOT Act was critical to the Department's ability to safeguard the Nation's security by bringing criminal charges against Al-Arian and others in February 2002.

~From the enactment of FISA in 1978 through September 11, 2001, available records indicate that Attorneys General issued 47 emergency authorizations for electronic surveillance and/or physical searches under FISA. Between September 11, 2001 and September 19, 2002, the Attorney General made 113 emergency authorizations for electronic surveillance and/or physical searches under FISA.

~The FBI has hired 264 new translators to support counterterrorism efforts, including 121 Arabic and 25 Farsi speakers.

~Section 212 (which allows computer-service providers to disclose communications and records of communications to protect life and limb) has been used to disclose vital information to law enforcement on many occasions, including one case where such records enabled agents to trace kidnappers' communications. This provision also proved invaluable in the investigation of a bomb threat against a school. An anonymous person, claiming to be a student at a high school, posted on an Internet message board a bomb death threat that specifically named a faculty member and several students. The owner and operator of the Internet message board turned over evidence that led to the timely arrest of the individual

responsible for the bomb threat. Faced with this evidence, the suspect confessed to making the threats.

~Section 216 was employed in the investigation of the murder of journalist Daniel Pearl to obtain information that proved critical to identifying some of the perpetrators.

~The Government's success in preventing another catastrophic attack on the American homeland in the 20 months since September 11, 2001, would have been much more difficult, if not impossibly so, without the USA PATRIOT Act. The Department's overall experience is that the authorities Congress provided in the Act have substantially enhanced our ability to prevent, investigate, and prosecute acts of terrorism.

~An informal survey of 45 FBI field offices reveal that fewer than ten of those offices have conducted investigative activities at mosques since September 11, 2001.

~The Department does not maintain centralized statistics on how many times agents attend public meetings.

~Every single person detained as a material witness as part of the September 11 investigation has been represented by counsel.

~Every single person detained as a material witness as part of the September 11 investigations was found by a federal judge to have information material to the grand jury's investigation.

~Each of the detained material witnesses is free to identify himself publicly.

~As of January 2003, the total number of material witnesses detained in the course of the September 11 investigation was fewer than 50.

~Approximately 90% of these material witnesses were detained for 90 days or less.

~The Attorney General has ordered the monitoring of attorney communications for a single inmate: Sheik Omar Ahmad Rahman, who was convicted for his part in the 1993 plot to bomb the World Trade Center. Rahman and his attorney were notified that their communications were subject to monitoring. No monitoring has occurred, however, because the inmate and his attorneys thus far have chose not to communicate further with each other.

The following additional information was indicated in the Department's response:

~The Department has used the new powers of the PATRIOT Act for non-terrorism cases (drug violations, credit card fraud, theft from a bank account, a lawyer who defrauded his clients).

~The Department has sought and the courts have authorized delayed notification of search warrants 47 times. Some courts have authorized delayed notification lasting until the indictment was unsealed. The Department has sought extensions of such delayed notifications 248 times.

~The Attorney General made emergency authorizations 113 times for FISA electronic

surveillance and/or physical searches in a one-year period.

~A December 24, 2002 memorandum from the Deputy Attorney General and the FBI Director providing guidance on the use of FISA to US Attorneys and all FBI agents says that FISA can be used as long as there is a significant "non-prosecutorial" purpose.

~Prior to moving to DHS, the INS did not charge any aliens with the expanded terrorism grounds of inadmissibility or deportability provided under section 411 of the PATRIOT Act.

b6
b7C

From:
Sent: Monday, August 04, 2003 11:38 AM
To:

Subject: FW: New Executive Order Re Information Sharing

FYI. I filed the Exec Ord. in elec lib

b6
b7C

-----Original Message-----
From:
Sent: Monday, August 04, 2003 11:35 AM
To:

Subject: FW: New Executive Order Re Information Sharing

b6
b7C

b6
b7C

-----Original Message-----
From:
Sent: Monday, August 04, 2003 11:28 AM
To:

Cc:
Subject: New Executive Order Re Information Sharing

Hi everyone,

Attached is a new Executive Order 13311, titled, **"Homeland Security Information Sharing,"** dated July 29, 2003. Section 892 of the Homeland Security Act, which is referred to in this EO,

specifically concerns Facilitating Homeland Security Information Sharing Procedures http://30.100.99.18/ogc/library/Homeland/home.pdf

I have also attached a law review article titled, "THE USA PATRIOT ACT'S APPLICATION TO LIBRARY RECORDS." Unsurprisingly, the law student who wrote this article comes down against the Government and our authority to search library patron records under the PATRIOT Act. *See* section 215 USA PATRIOT Act, codified at 50 USC 1861-1862 (attached).

Speaking of accessing library records, Senator Russ Feingold introduced legislation last week (The Library Bookseller and Personal Records Privacy Act) that would limit the FBI's authority to search library records, etc. . . *See attached*

Please forward to all appropriate units/squads.


EO 13311 formation sharing.w


library records PATRIOT Act.wp...


50 USC 1861.wpd (13 KB)


50 USC 1862.wpd (10 KB)


Feingold Introduces Legislatio...


getdoc.cgi_dbname =108_cong_bil...

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

From [redacted] (OGC) (FBI)
Sent: Wednesday, October 06, 2004 4:30 PM
To: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI)
Subject: RE: Business Records/Health Care industry

b5
b6
b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 10-04-2005 BY 65179 DMH/JHF 05-CV-0845

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

b6
b7C

[redacted] I don't think this is ALU turf. ILU has the turf on health records for criminal cases. So I'm sending this to [redacted] in ILU. Also to NSLB's own [redacted] recently in ILU.

-----Original Message-----
From [redacted] (OGC) (FBI)
Sent: Wednesday, October 06, 2004 3:23 PM
To: [redacted] (OGC) (FBI)
Subject: FW: Business Records/Health Care industry

b5
b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]

Thanks. [redacted]

b6
b7C

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Wednesday, October 06, 2004 3:17 PM
To: BOWMAN, MARION E. (OGC) (FBI); [redacted] (OGC) (FBI) [redacted] (OGC) (FBI)
Subject: RE: Business Records

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

b6
b7C

[redacted] Why don't you touch base with ALU on this as well just to come up to speed on health records. Ask [redacted] who he has covering this now.

-----Original Message-----
From: BOWMAN, MARION E. (OGC) (FBI)
Sent: Wednesday, October 06, 2004 11:26 AM
To: [redacted] (OGC) (FBI) [redacted] (OGC) (FBI); [redacted] (OGC) (FBI)
Subject: RE: Business Records

b5
b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]

[redacted]

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b6
b7C

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Wednesday, October 06, 2004 11:22 AM
To: BOWMAN, MARION E. (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI)
Subject: Business Records

b5
b6
b7C
b7D

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]

SENSITIVE BUT UNCLASSIFIED

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

SENSITIVE BUT UNCLASSIFIED

RE RE RE FW Director's 723 Senate Hearing.txt

From: [redacted] b6 b7C
Sent: Wednesday, July 16, 2003 12:52 PM
To: [redacted]
Cc: [redacted] Rowan, J Patrick; [redacted]
Subject: RE: RE: RE: FW: Director's 7/23 Senate Hearing

[redacted] - here are the top picks from me and Bill. There is no particular order of importance among these: b6 b7C

Privacy Act:

1. Section 552a(a)(8)(B) is amended by adding the following new subsection:

"(ix) matches performed by, or at the request of, an agency (or component thereof) which performs as a principal function any activity pertaining to national security (including the prevention of terrorism), for purposes relating to national security (including the prevention of terrorism)." b5

[redacted]

2. Section 552a(e)(6) is amended by adding the following after "section": "or pursuant to a counterterrorism or national security matter." b5

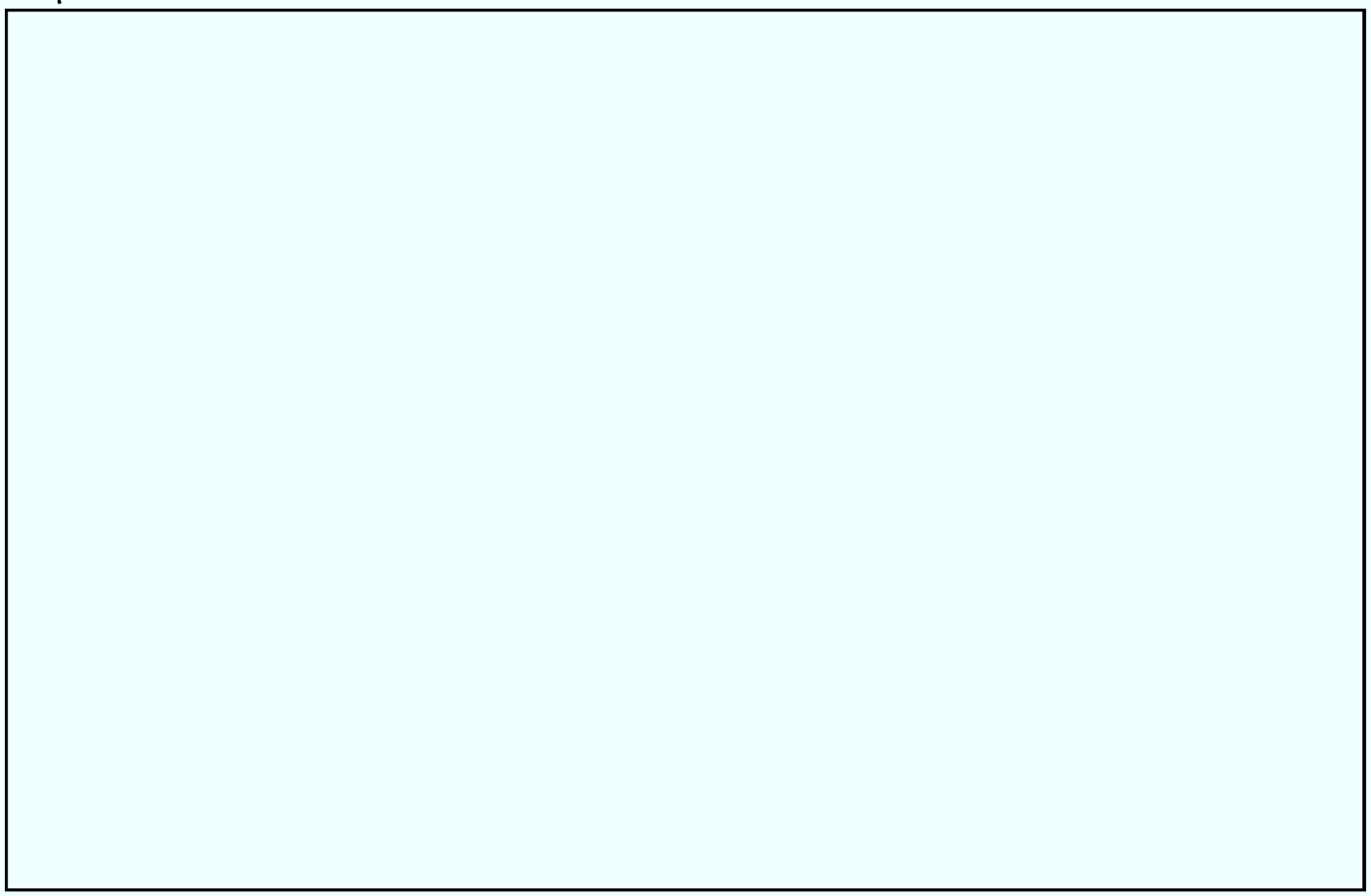
[redacted]

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

counterterrorism and national security matters.

3. Section 552a(g) of title 5, United States Code, is amended by adding at the end the following new paragraph:

"(6) If the head of an agency exempts a system of records from this subsection as provided in subsection (j), no court shall have jurisdiction over any civil action brought against said agency for failure to comply with any provision of this Act." b5



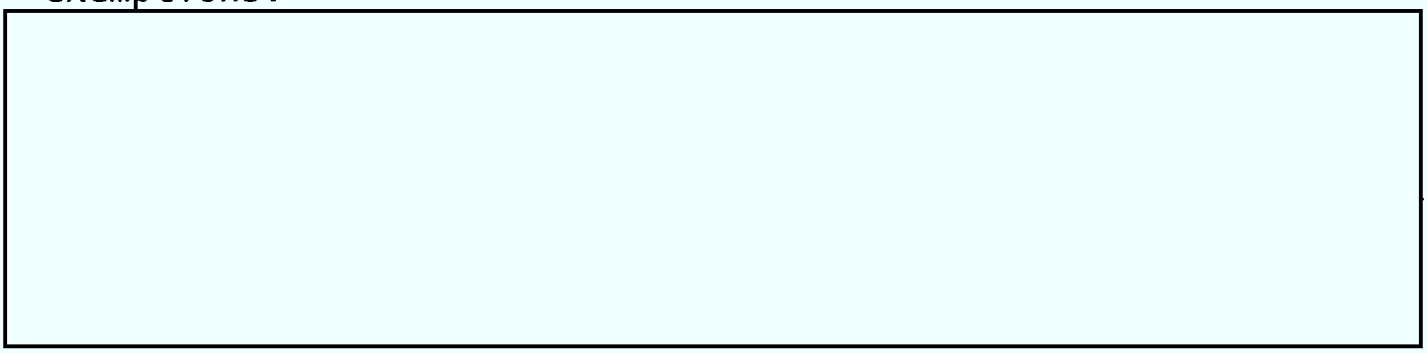
4. Section 552a(j) is amended by adding the following sentence to the end of the section:

"The statement of reasons for such exemptions shall not, however, constitute a limitation on the scope of the exemptions."

Why? This amendment is intended to reverse case law which suggests that the statement of reasons for the exemptions constitutes a limitation on the scope of the exemption. While agencies are required to publish the reasons why a system of records is to be exempted from a provision of the Act, agencies should not have to divine all possible reasons at the time of publication at the risk that such failure could be exploited by terrorists or others.

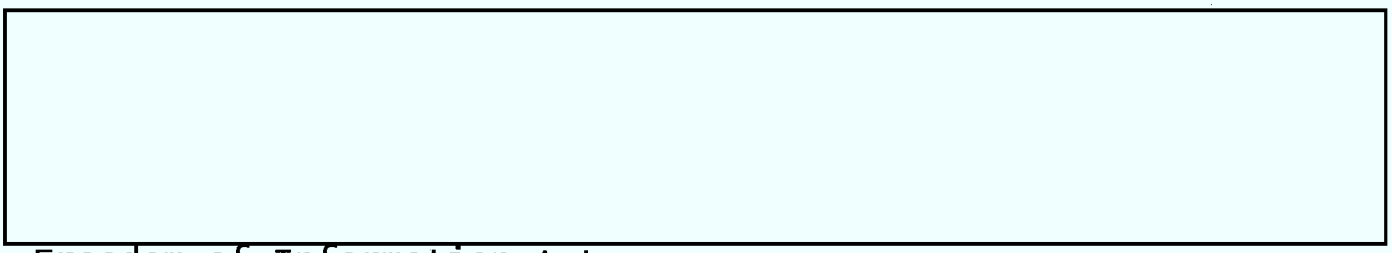
5. Section 552a(k) is amended by adding the following sentence to the end of the section:

"The statement of reasons for such exemptions shall not, however, constitute a limitation on the scope of the exemptions." b5



6. Section 552a(j)(1) is amended by striking the semi-colon and the word "Agency" and adding the following:

"or the Federal Bureau of Investigation." b5



Freedom of Information Act

1. Section 552(a)(3)(A) of title 5, United States Code, is amended by adding the following at the end:

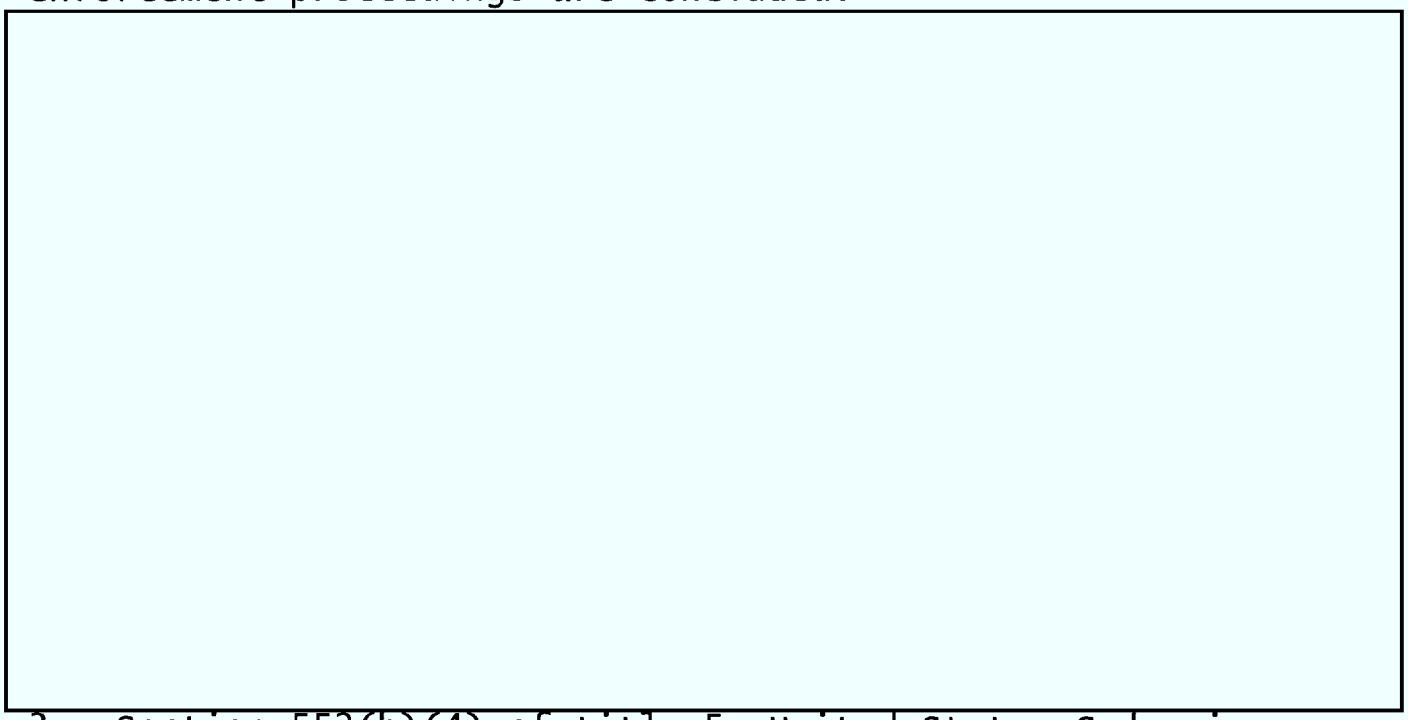
"The provisions of this paragraph shall not apply to requests submitted to agencies involved in national security, counterterrorism, homeland security or border

security matters by or on behalf of (i) foreign persons, except lawful permanent residents, or (ii) persons suspected of engaging in or supporting terrorism, foreign intelligence collection, or other activities inimical to the national security interests of the United States. As relating to records of the agencies described above, requests need not be processed, nor need any response be provided to any person, except upon a written certification of such person, subject to the penalties of 18 U.S.C. 1001, stating that person's true name and address and that the person has no knowledge or reason to belief that the request is being submitted by or on behalf of any of the persons described above. In addition to or in lieu of any criminal prosecution, the Attorney General may bring a civil action against any person who seeks or obtains records in violation of this paragraph. The court in which such action is brought may assess against such person a penalty in any amount not to exceed $100,000. Such remedy shall be in addition to any other remedy available under statutory or common law.." b5

agencies to devote limited resources to activities such as homeland security that are essential to the citizenry. This amendment will prohibit such individuals or their representatives from making FOIA requests to agencies involved in national security, counterterrorism, homeland security or border security matters. These changes will not impair due process of the persons affected because they will still retain all of the discovery rights that are otherwise available in the forum in question.

2. Section 552(b)(7) of title 5, United States Code, is amended by adding the following at the end of the last paragraph:

"An agency's claim of exemption based solely on (b)(7)(A) shall not constitute a bar to or waiver of the claim of any other exemption in this section once the enforcement proceedings are concluded." b5



3. Section 552(b)(4) of title 5, United States Code, is amended to read as follows:

"(b)(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential. In addition, any agency may delay, for a

period not to exceed 5 years after development, the unrestricted public disclosure of technical data that could have qualified as a trade secret or commercial or financial information that is privileged or confidential if the information had been obtained from a non-Federal party, in any case in which the technical data is generated in the performance of experimental, developmental, research, counterterrorism or national security activities or programs, conducted by, or funded in whole or in part by, the agency. Such technical data referred to in this subsection shall not be subject to the disclosure requirements of this section. This paragraph shall in no way affect the applicability of any other provision of this subsection."

b5

[redacted]

-----Original Message-----
From: [redacted]
Sent: Wednesday, July 16, 2003 9:31 AM
To: [redacted]
Cc:
Subject: Re: RE: RE: FW: Director's 7/23 Senate Hearing

b6
b7C

b5

[redacted]

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

RE RE RE FW Director's 723 Senate Hearing.txt [redacted] b5

Thanks for this follow up. -[redacted] b5 b6 b7C

[redacted] 07/16 9:14 AM >>>

>>>

[redacted]

-----Original Message-----

From: [redacted] b6 b7C

Sent: Tuesday, July 15, 2003 1:51 PM

To: [redacted]

Cc:

Subject: Re: RE: FW: Director's 7/23 Senate Hearing

[redacted] b5 b6 b7C

[redacted]:

Thanks.

[redacted]

b5

[redacted]

[redacted]
Office of Congressional Affairs
Room 7252, JEH Bldg
[redacted]

b6
b7C
b2
b5
b6
b7C

>>> [redacted] 07/15 12:55 PM >>>

[redacted]

-----Original Message-----
From: [redacted]
Sent: Monday, July 14, 2003 12:23 PM
To: [redacted]
[redacted]
Cc: Steele, Charles M; [redacted]
[redacted] Kelley, Patrick W
Subject: Re: FW: Director's 7/23 Senate Hearing

b6
b7C

b5
b6
b7C

[redacted]

b2
b5
b6
b7C

RE RE RE FW Director's 723 Senate Hearing.txt

[redacted]

Thanks for playing our game!

--[redacted](ext. [redacted])

>>>[redacted]07/14 11:06 AM >>>

[redacted]

-----Original Message-----
From: [redacted]
Sent: Sunday, July 13, 2003 8:27 PM
To: Kelley, Patrick W
Cc: [redacted] Kalisch, Eleni P.; [redacted] Rowan, J Patrick; [redacted] Bowman, Marion E; [redacted]
Subject: Director's 7/23 Senate Hearing

b5
b6
b7C
b5
b6
b7C

[redacted]

b5

b5

[redacted]

[redacted]

Office of Congressional Affairs
Room 7252, JEH Bldg

b2
b6
b7C

b6
b7C

From:
Sent: Thursday, January 22, 2004 12:28 PM
To: Caproni, Valerie E.; Curran, John F; KELLEY, PATRICK W.;
Cc:
Subject: DNA issue--change in meeting to Tuesday

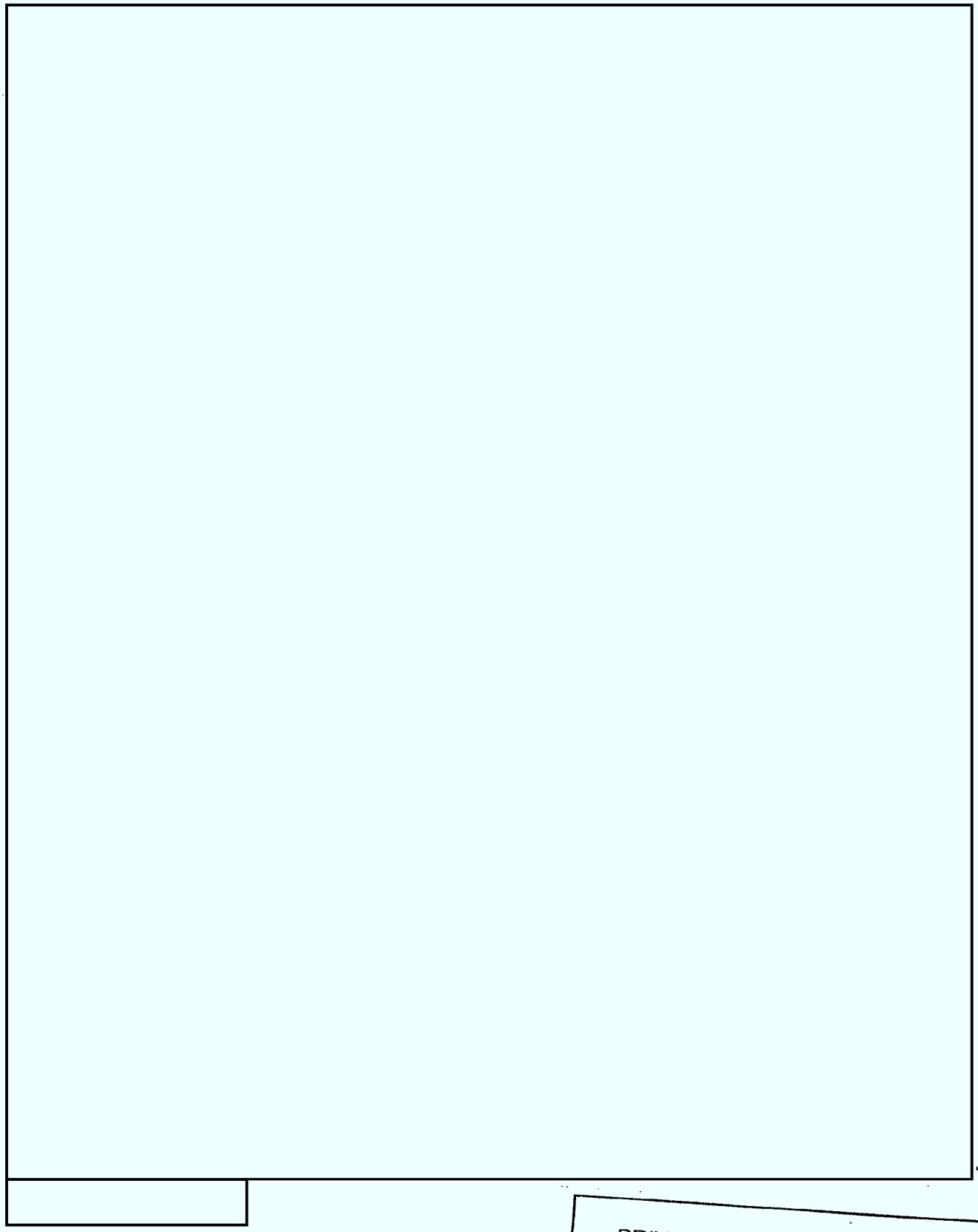
b5
b6
b7C

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5
b6
b7C

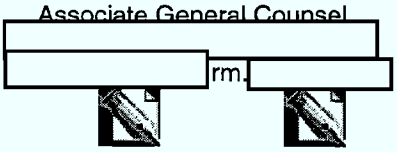
PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5
b6
b7C



PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

Associate General Counsel



labafipmou.ec.w pd (31 KB)

requestfordnaby :ia2.ec.wpd (16..

b2
b6
b7C

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

From: [redacted] (Div09) (FBI)
Sent: Tuesday, May 04, 2004 6:35 PM
To: [redacted] (LD) (FBI)
Cc: [redacted]
Subject: RE: sharing DNA profiles with [redacted]

b6
b7C

b7D

b5
b6
b7C

UNCLASSIFIED
NON-RECORD

[redacted]

-----Original Message-----
From: [redacted] (LD) (FBI)
Sent: Tuesday, May 04, 2004 1:25 PM
To: [redacted] (Div09) (FBI)
Subject: FW: sharing DNA profiles with [redacted]

b6
b7C

b7D

UNCLASSIFIED
NON-RECORD

b6
b7C

Hi [redacted]

[redacted] b5 b6 b7C

Thanks -
[redacted]

-----Original Message-----
From: [redacted] b6
Sent: Wednesday, April 07, 2004 1:47 PM b7C
To: [redacted] (Div09) (FBI)
Subject: sharing DNA profiles with [redacted] b7D

Expires After: 7/6/2004 00:00

Hi [redacted]:

[redacted] b5 b6 b7C b7D

Thanks, [redacted]

UNCLASSIFIED

UNCLASSIFIED

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5
b6
b7C

-----Original Message-----**From** [redacted] (OGC) (FBI) **Sent:** Thursday, August 19, 2004 8:47 AM**To:** [redacted] (OGC) (FBI)**Cc:** [redacted] (OGC)(FBI)**Subject:** RE: Discretionary Access Control Team

UNCLASSIFIEDNON-RECORD

[redacted]

-----Original Message-----**From:** [redacted] (OGC) (FBI) **Sent:** Wednesday, August 18, 2004 6:41 PM**To:** [redacted] (OGC) (FBI)**Cc:** [redacted] (OGC)(FBI)**Subject:** RE: Discretionary Access Control Team

b5
b6
b7C

UNCLASSIFIEDNON-RECORD

[redacted]

-----Original Message-----**From:** [redacted] (OGC) (FBI) **Sent:** Wednesday, August 18, 2004 5:46 PM**To:** [redacted] (OGC) (FBI)**Cc:** [redacted] (OGC)(FBI); KELLEY, PATRICK W. (OGC) (FBI); Curran, John F. (OGC) (OGA); [redacted] (OGC) (FBI); BOWMAN, MARION E. (OGC) (FBI)**Subject:** RE: Discretionary Access Control Team

b5
b6
b7C

UNCLASSIFIEDNON-RECORD

[redacted]

-----Original Message-----**From** [redacted] (OGC) (FBI) **Sent:** Wednesday, August 18, 2004 1:35 PM**To:** KELLEY, PATRICK W. (OGC) (FBI); Curran, John F. (OGC) (OGA); [redacted] (OGC) (FBI) [redacted] (OGC) (FBI); BOWMAN, MARION E. (OGC) (FBI)**Cc** [redacted] (OGC)(FBI)**Subject:** FW: Discretionary Access Control Team

b5
b6
b7C

UNCLASSIFIEDNON-RECORD

[redacted]

-----Original Message-----**From:** [redacted] (OGC) (FBI) **Sent:** Wednesday, August 18, 2004 1:03 PM**To** [redacted] (OGC) (FBI)**Subject:** RE: Discretionary Access Control Team

b5
b6
b7C

UNCLASSIFIEDNON-RECORD

[redacted]

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

[redacted]

-----Original Message-----**From:** [redacted](OGC) (FBI) **Sent:** Wednesday, August 18, 2004 10:29 AM**To:** [redacted](OGC) (FBI)**Cc:** Curran, John F. (OGC) (OGA); BOWMAN, MARION E. (OGC) (FBI); [redacted](OGC) (FBI); KELLEY, PATRICK W. (OGC) (FBI); [redacted]OGC)(FBI); [redacted](OGC) (FBI)**Subject:** FW: Discretionary Access Control Team

b5
b6
b7C

UNCLASSIFIEDNON-RECORD

[redacted]

-----Original Message-----**From:** [redacted](OI) (OGA) **Sent:** Wednesday, August 18, 2004 8:57 AM**To:** VAN DUYN, DONALD N. (CTD) (FBI); LAUGHLIN, LAURA M. (CID) (FBI); BOLLINGER, VIRGINIA L. (CD) (FBI); SEAVEY, GAIL M. (CyD) (FBI); [redacted](SecD) (OGA)[redacted](OGC) (FBI); [redacted](OI) (FBI)**Cc:** [redacted](ITOD)(FBI); [redacted](ITOD)(FBI); [redacted](CTD) (FBI); [redacted](OGC) (FBI); BERNAZZANI, JAMES (OI) (FBI); BAGINSKI, MAUREEN A. (DO) (FBI); BROCK, KEVIN R. (CI) (FBI); [redacted](DO) (FBI); AZMI, ZALMAI (OCIO) (FBI)[redacted](SecD) (FBI)**Subject:** Discretionary Access Control Team

b6
b7C

UNCLASSIFIEDNON-RECORD

[redacted]

b5

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

[redacted]

b5
b6
b7C
b2

Thanks,

[redacted]

Office of Intelligence [redacted]

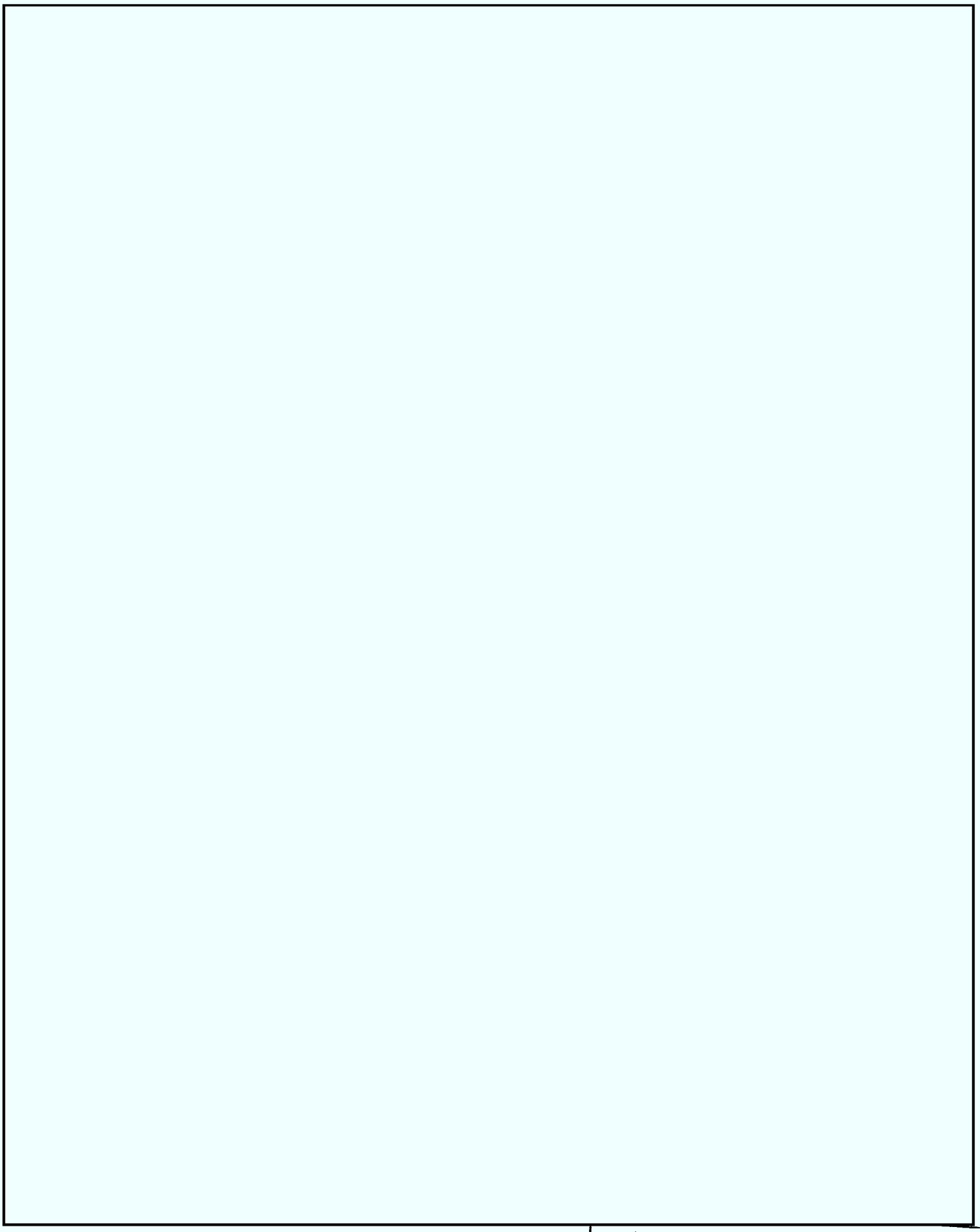
PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

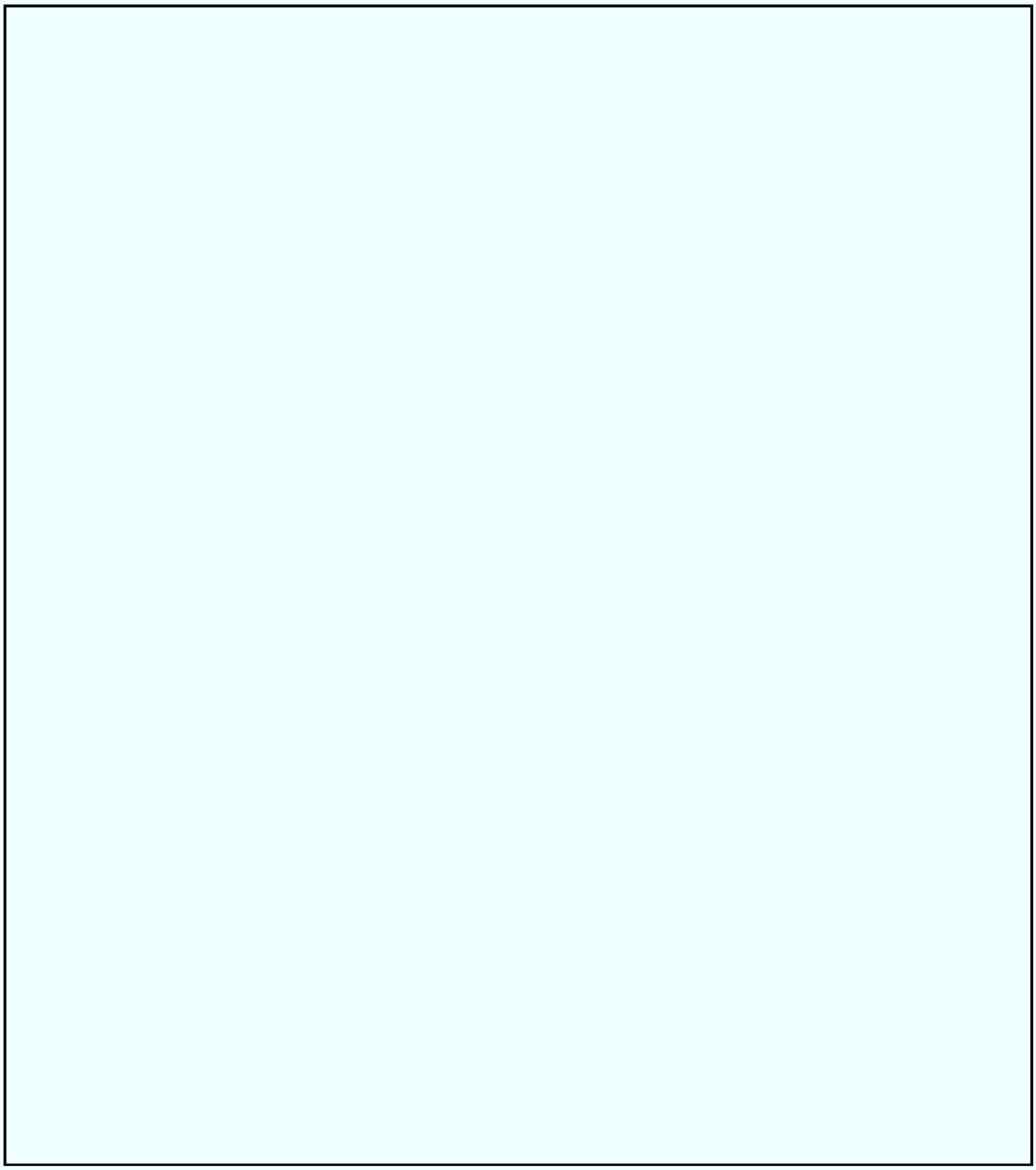
RESTRICTIONS AND CONDITIONS ON DISCLOSING FBI INFORMATION FROM INTERNATIONAL TERRORISM (315) INVESTIGATIONS TO THE NATIONAL COUNTER-TERRORISM CENTER AND OTHER COMPONENTS OF THE INTELLIGENCE COMMUNITY

b5

I. RESTRICTIONS BASED ON THE TYPE OF CRIMINAL LEGAL PROCESS

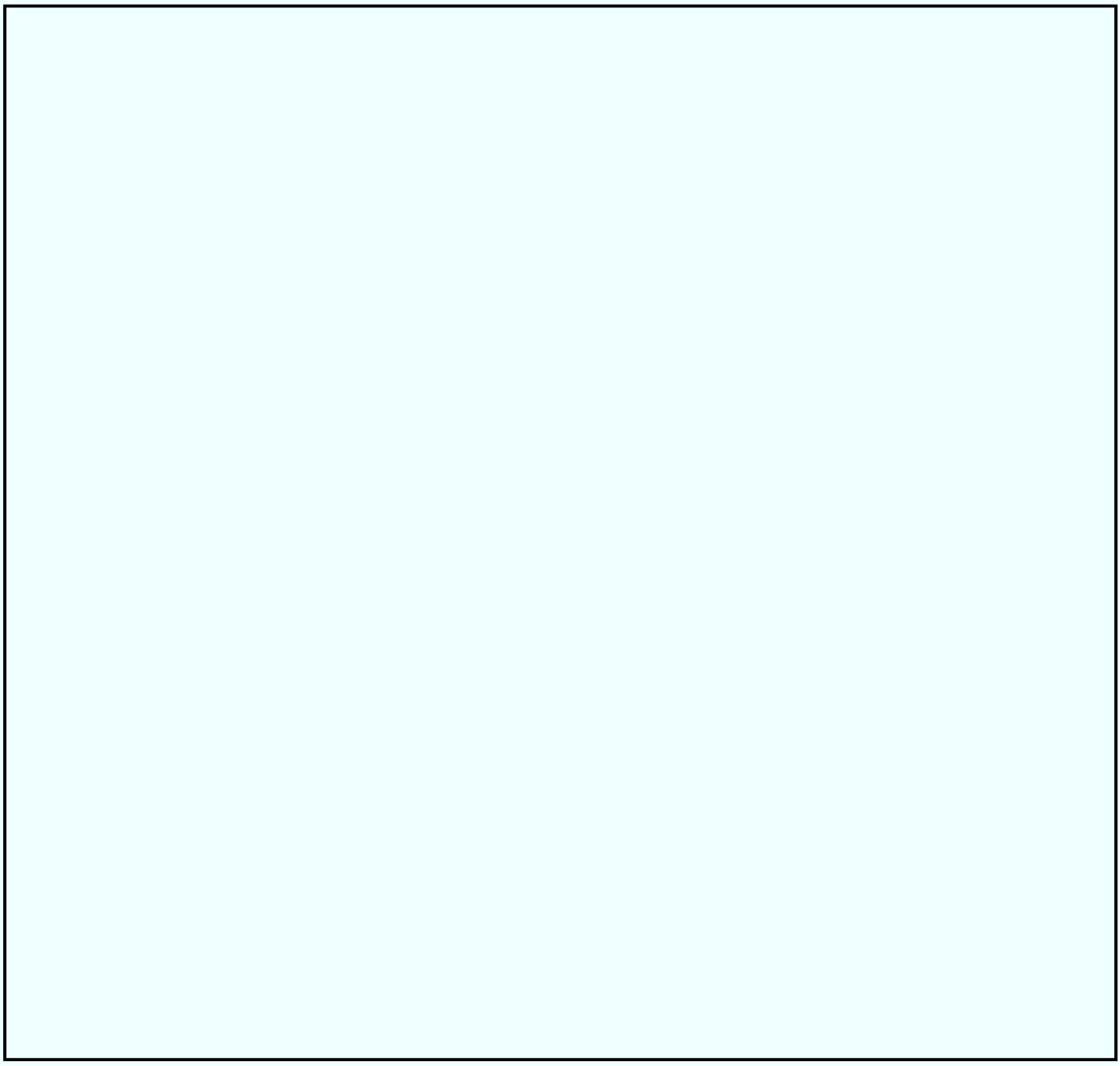
b5



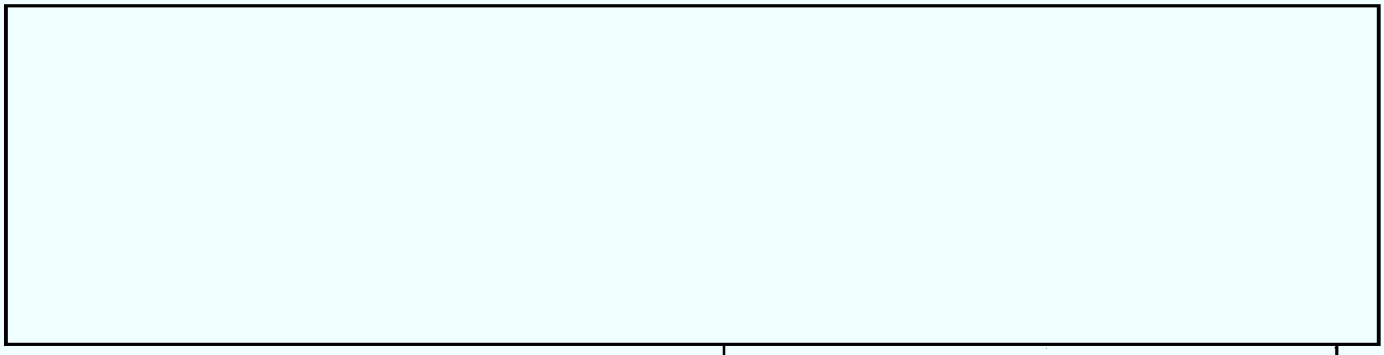


PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5

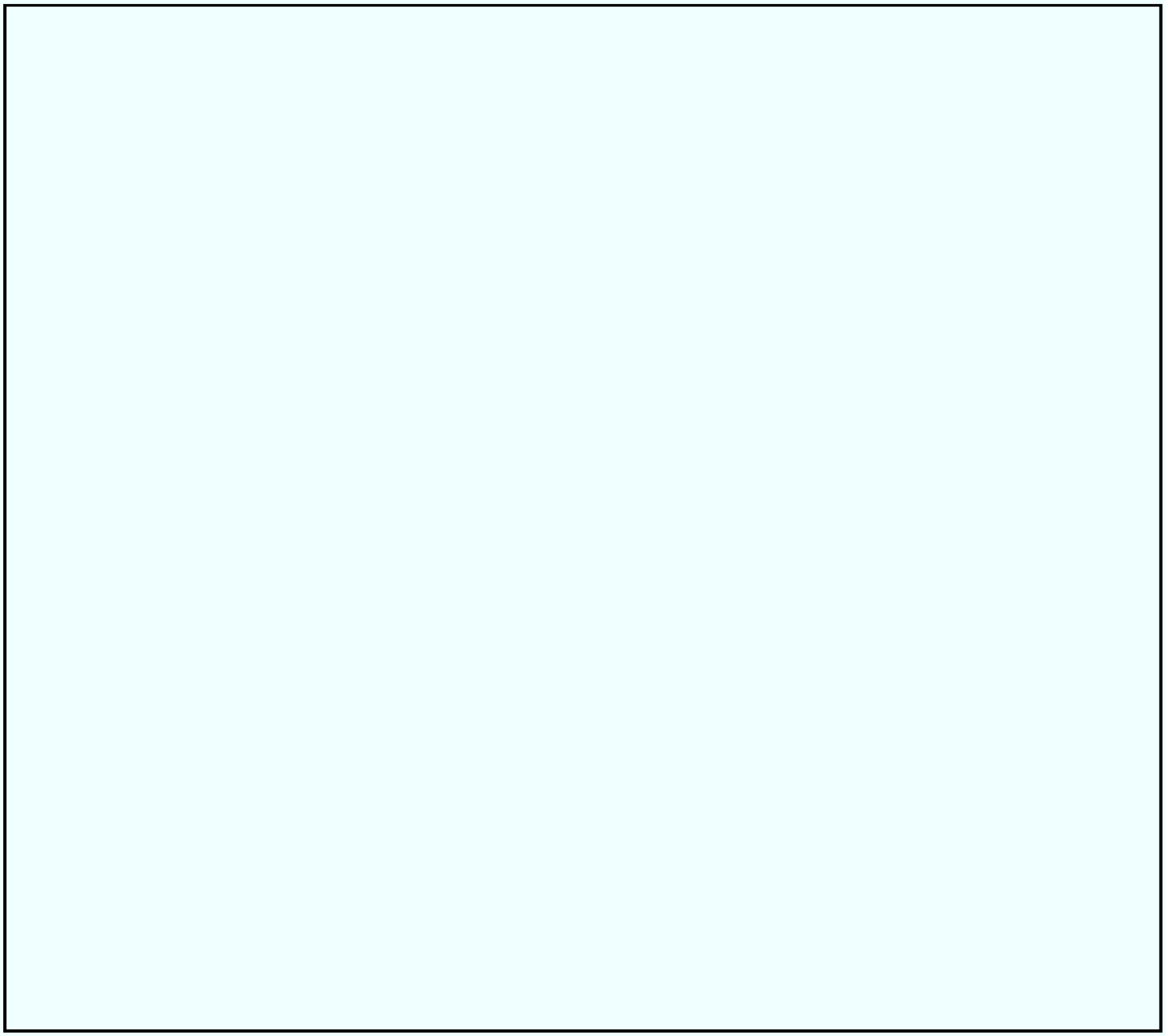


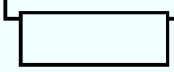
b5



PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

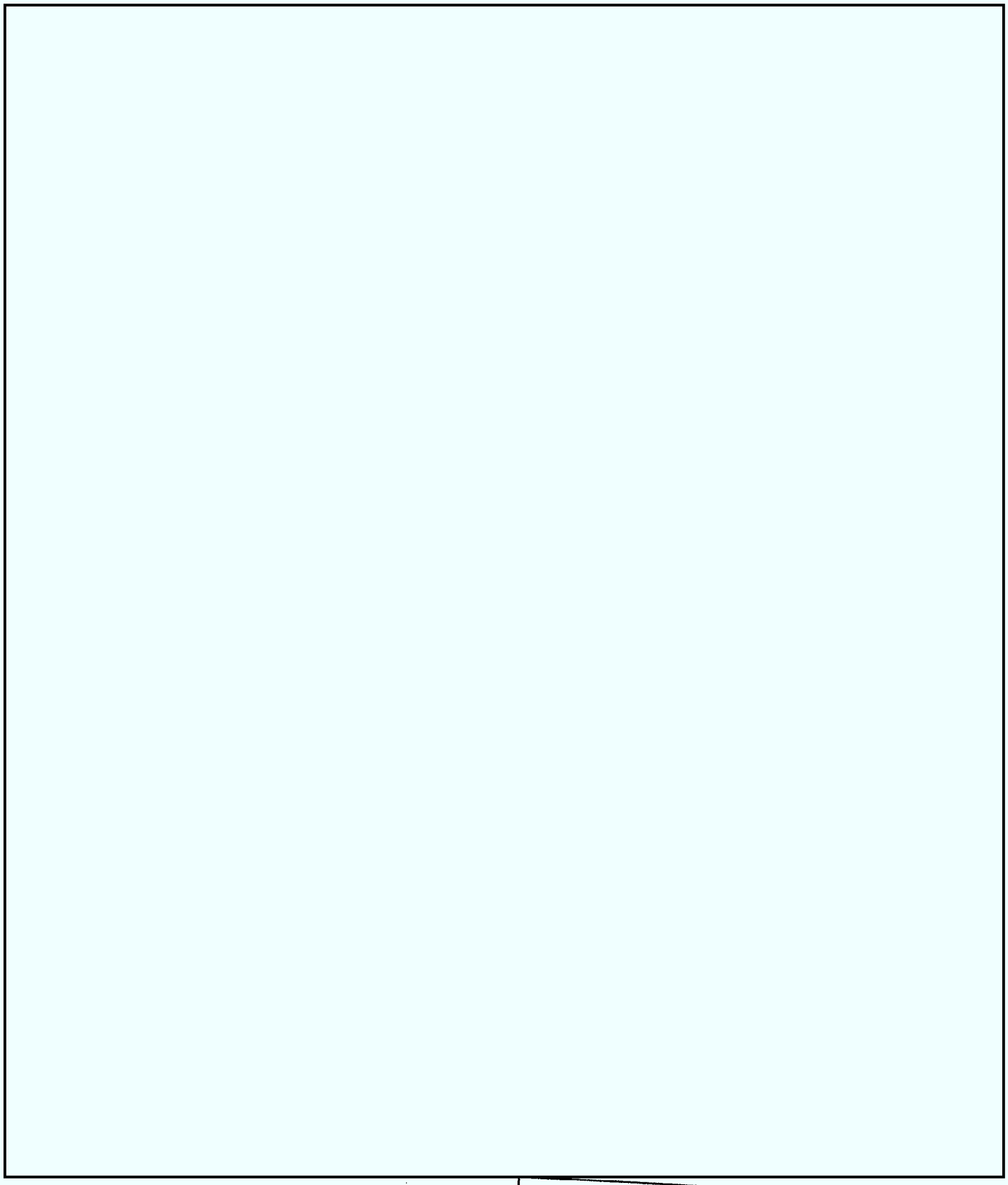
b5





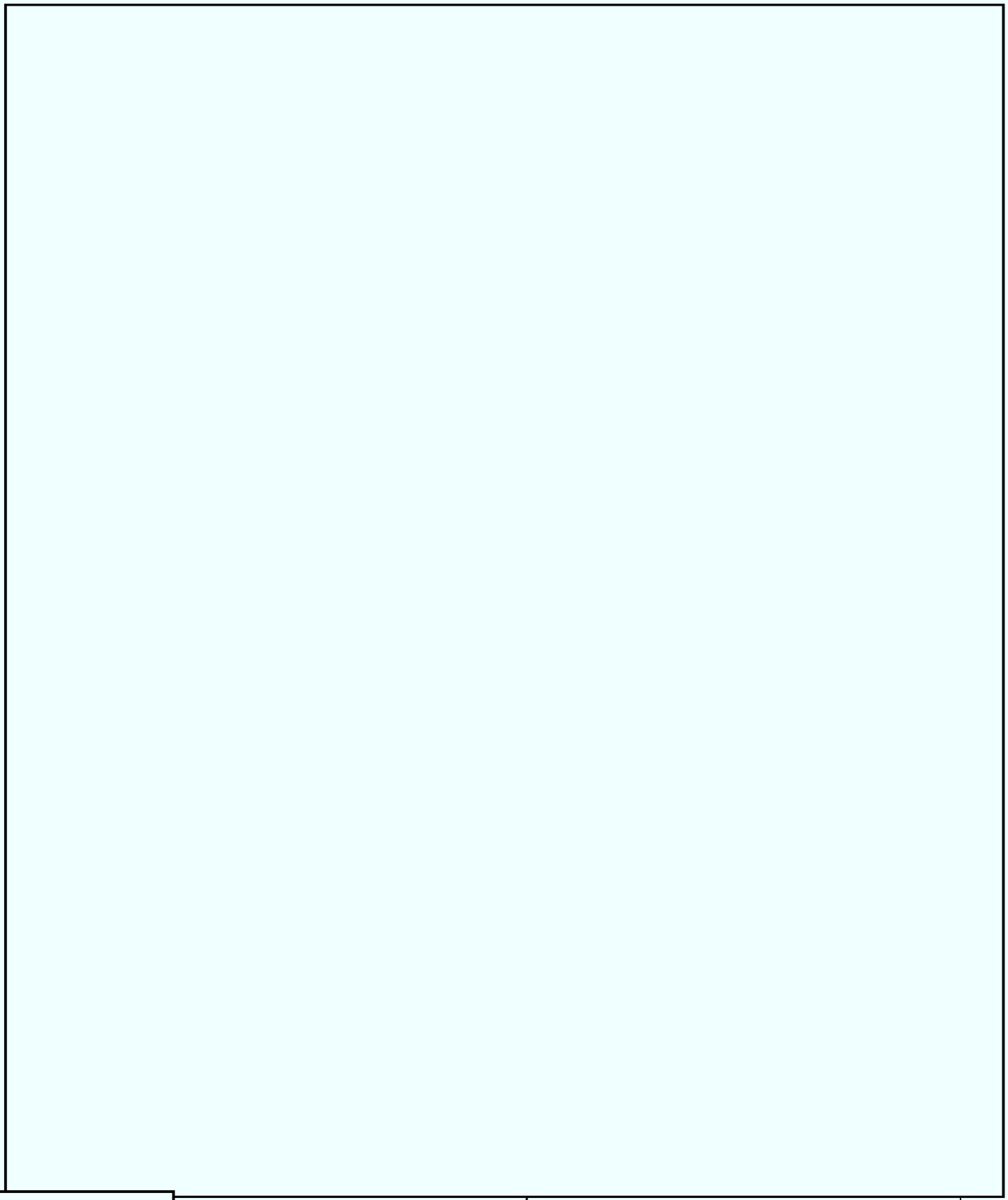
b5

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT



PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT



b5

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

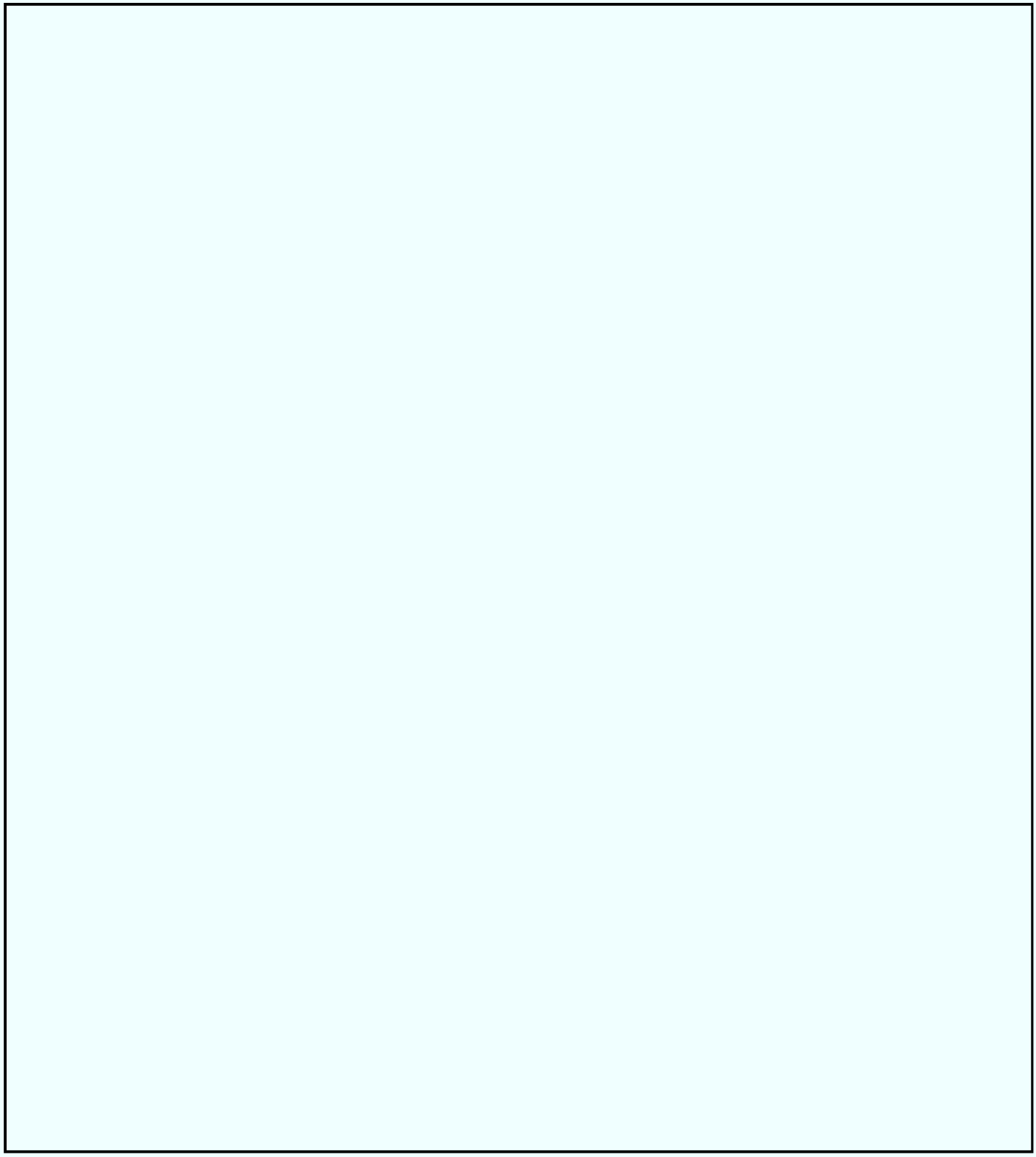
b5

7

Disclosure to the TTIC of Criminal Information obtained in International Terrorism (315) Cases

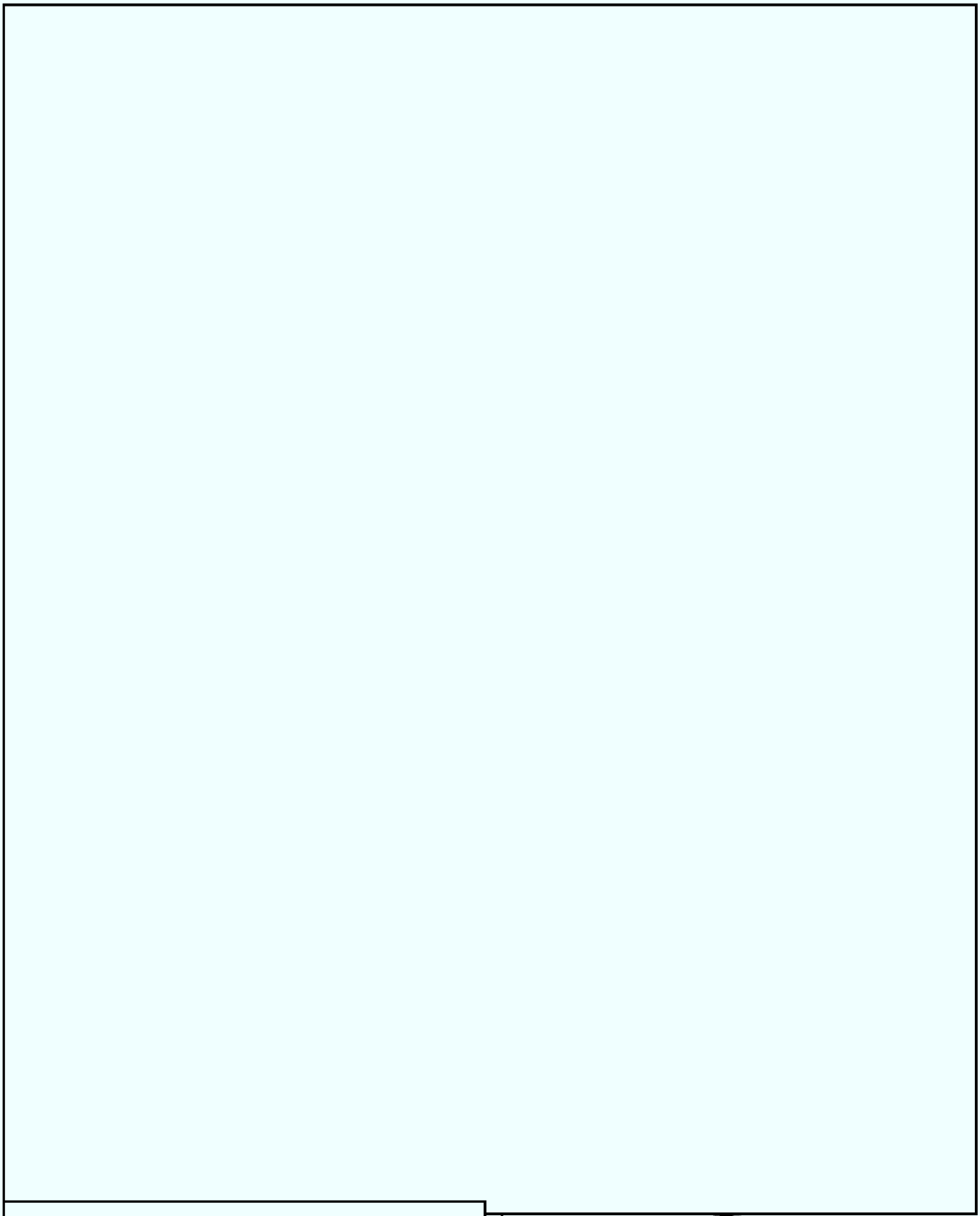
PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

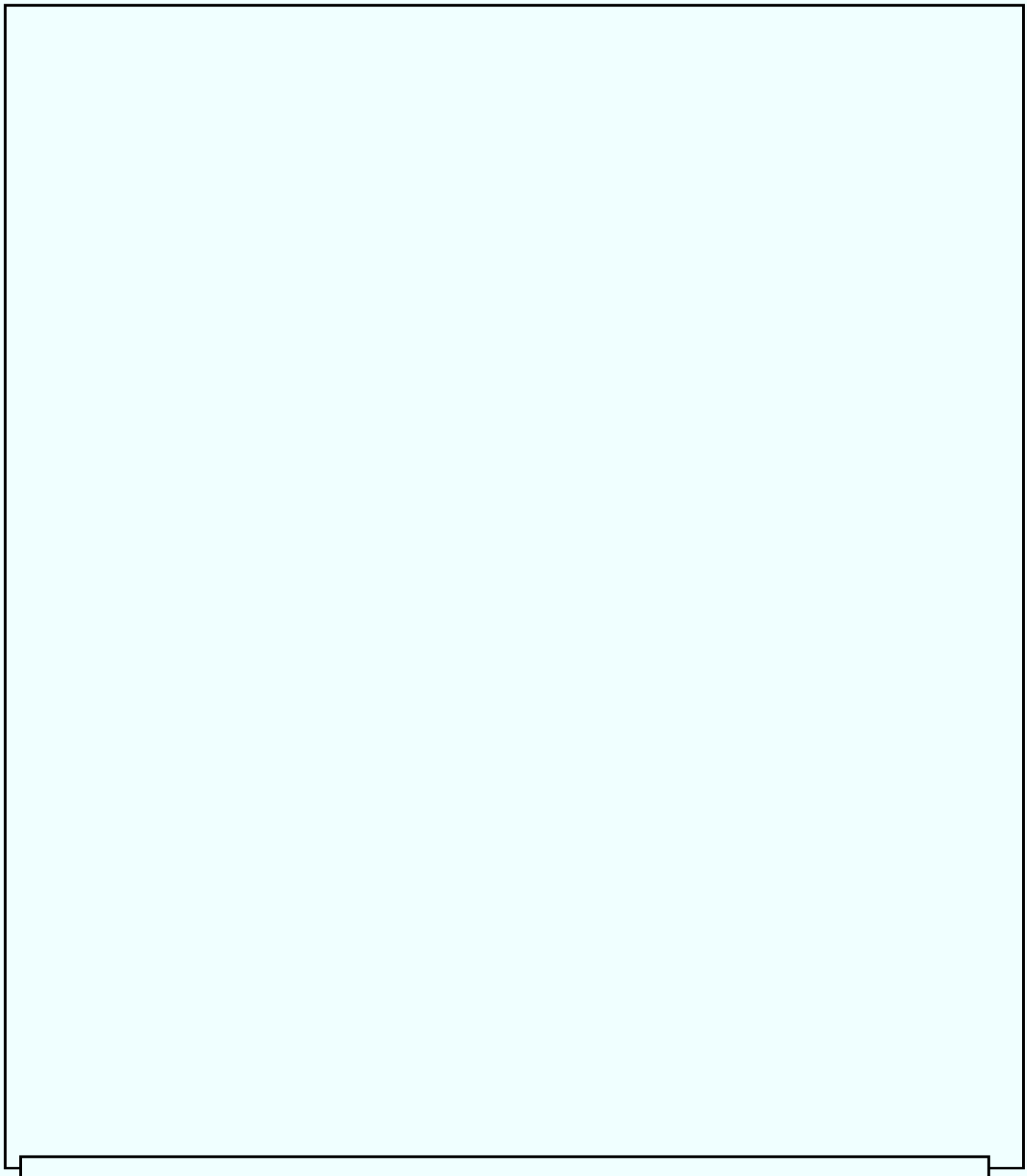
b5

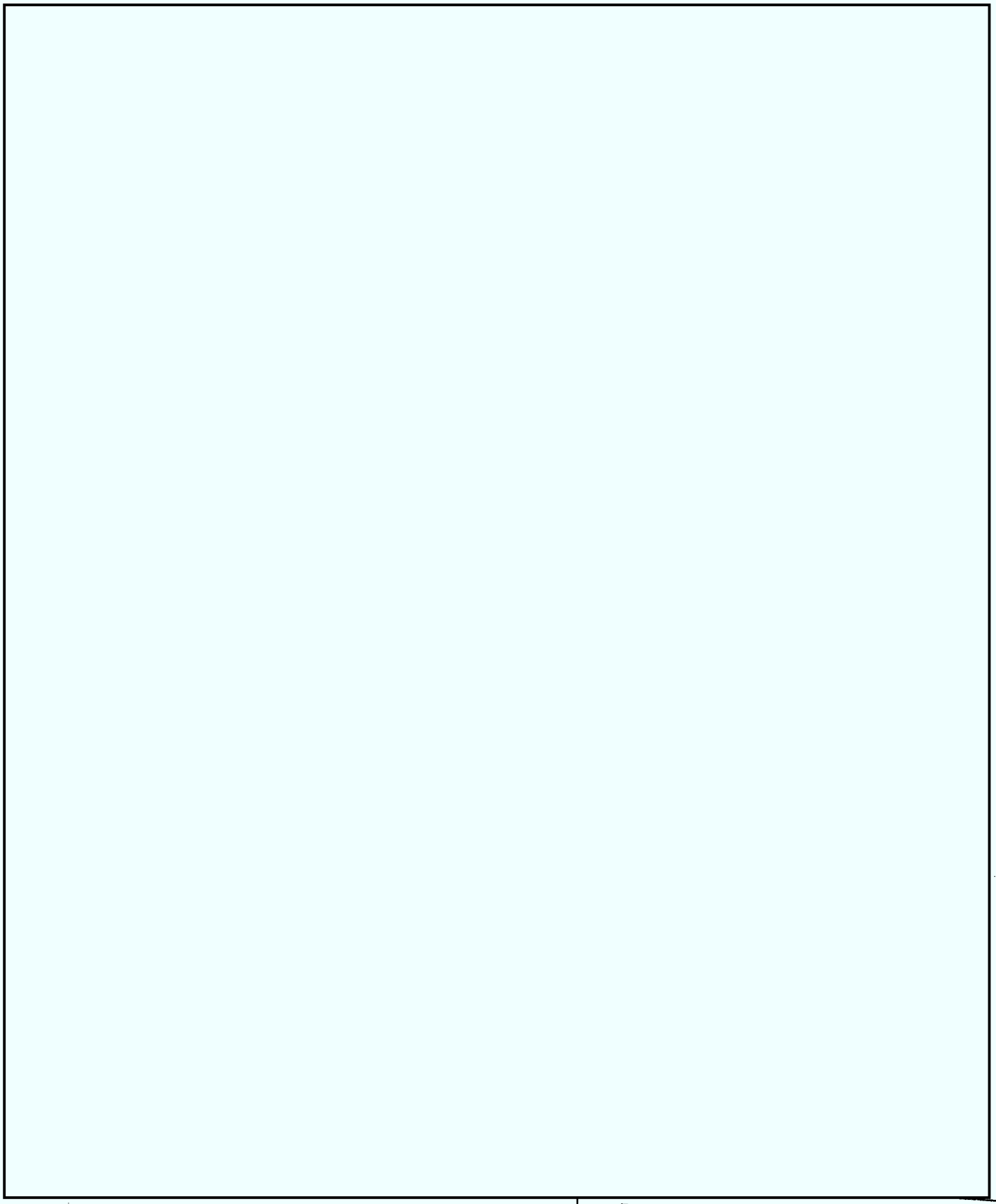


b5

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

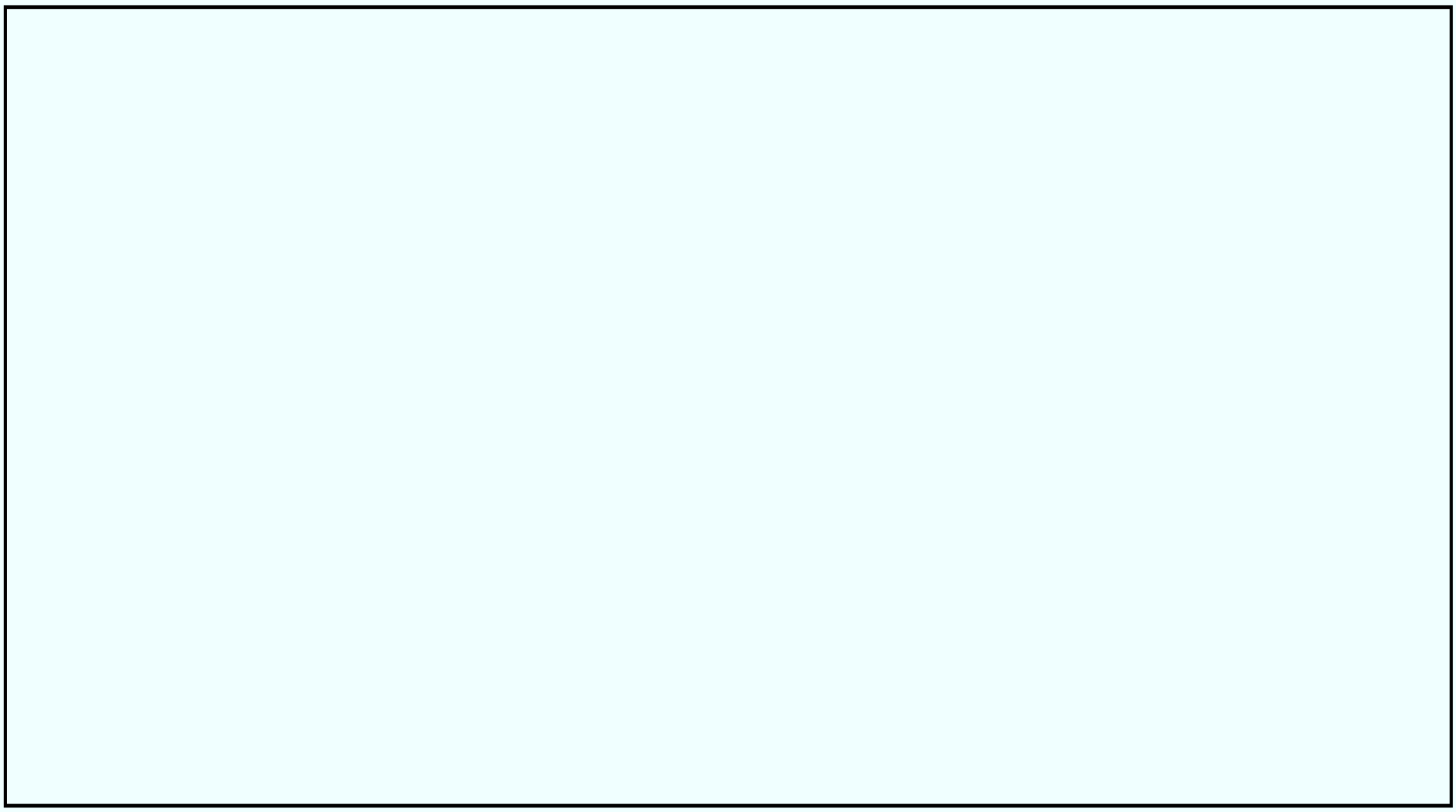






b5

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT



b5

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

7

To: All Divisions From: Office of the General Counsel
Re: 66F-HQ-A1247863, 10/26/2001

DATE: 12-09-2005
CLASSIFIED BY 65179 DMH/LP 05-CV-0845
REASON: 1.4 ((C))
DECLASSIFY ON: 12-09-2030

From: Office of the General Counsel
NSLU/NSLB, Room 7975
Contact: National Security Law Unit, [redacted] b2

Approved By: Mueller Robert S III
Pickard Thomas J
Parkinson Larry R
Bowman M E
[redacted] b6 b7C

Drafted By: [redacted] mjw

Case ID #: 66F-HQ-A1247863 (None)

Title: NEW LEGISLATION
REVISIONS TO FCI/IT LEGAL AUTHORITIES
FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA)

Synopsis: Summarizes recent changes to FISA statute and related legal authorities.

Details:

Background

On October 26, 2001, the President signed the "Uniting and Strengthening America Act by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001" which significantly revises many legal authorities relating to counterterrorism. The Act, which consists of more than 150 sections, effects changes in national security authorities, the substantive criminal law, immigration law, money laundering statutes, victim assistance statutes, and other areas [redacted] b5

[redacted]

~~SECRET~~

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5

[redacted]

1. Sharing Grand Jury, Title III and Criminal Investigative Information

Section 203 first amends Federal Rule of Criminal Procedure 6(e) to permit the disclosure of grand jury information involving intelligence information "to any Federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to assist the official receiving that information in the performance of his official duties." The Section also requires subsequent notice to the Court of the agencies to which information was disseminated and adds a definition of "foreign intelligence information" to Rule 6(e). The Grand Jury portion of this Section (Section 203(a)) is not subject to the sunset provision.

Section 203 then amends Title III to allow the same sort of disclosure of Title III information when the matters involve foreign intelligence "to any other Federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to assist the official receiving that information in the performance of his official duties." The Section adds a definition of foreign intelligence information to Title III, and requires the Attorney General to develop procedures for the sharing of Grand Jury or Title III information that identifies a U.S. person.

Finally, Section 203 establishes that "notwithstanding any other law" it is lawful for criminal investigators to share foreign intelligence information obtained in the course of a criminal investigation with any other Federal law enforcement, intelligence, protective, immigration, national defense, or national security official, as above.

The intent of Section 203 is to eliminate barriers to the timely sharing of information between criminal investigators and other entities (the Intelligence Community, the INS, DoD, etc.) involved in the protection of the national security. The Section essentially gives the FBI full discretion to share criminal investigative information, regardless of its source, whenever it involves foreign intelligence information (which is defined to include all foreign intelligence, counterintelligence, and counterterrorism information).

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

Procedural Changes: FBI components in possession of information obtained through criminal investigative techniques that is also foreign intelligence information should arrange for the appropriate dissemination of the information. Dissemination to the Intelligence Community must be coordinated through the relevant NSD or CTD units at FBIHQ. When the DOJ issues procedures relating to the dissemination of U.S. person information, the field will receive additional guidance.

2. "Roving" FISA ELSUR Authority

Section 206 amends FISA to allow the Court to issue a "generic" secondary order where the Court finds that the "actions of the target of the application may have the effect of thwarting the identification of a specified person." This means that, when a FISA target engages in tradecraft designed to defeat ELSUR, such as by [redacted] the Court can issue an order directing "other persons, [redacted] etc., to effect the authorized electronic surveillance. Even if the target is not engaged in obvious tradecraft, we can obtain such an order as long as the target's actions may have the effect of thwarting surveillance. This will allow the FBI to go directly to the new carrier and establish surveillance on the authorized target without having to return to the Court for a new secondary order. [redacted]

b1 (S)

b5

Procedural Changes: When the field wants to obtain roving ELSUR authority, the request for a FISA sent to FBIHQ should include specific facts that will allow the Court to find that the actions of the target may have the effect of thwarting the requested surveillance, absent the roving authority. Such facts could include examples of previous tradecraft by the target, by members of the target's group or service, or by others with training or background similar to that presumed for the target. DOJ/OIPR may issue more detailed guidance as experience with this provision grows.

3. Changes in the Duration of FISA Authority

Section 207 extends the standard duration for several categories of FISA orders. First, the section allow for ELSUR and search orders on non-U.S. person agents of a foreign power pled under Section 101(b)(1)(A) of FISA (i.e., officers and employees of foreign powers, including members of international terrorist groups) to run for an initial period of 120 days (instead of 90) and to be renewed for periods of one year. The section also extends the standard duration of physical search orders in all other cases (U.S. persons and non-officer/employee targets) from 45 to 90 days.

Procedural Changes: None are required. OIPR will transition existing coverages to the new durations as they come up for renewal.

4. Expansion of the FISA Court

In order to increase the availability of FISA judges, Section 207 expands the Court from seven judges to eleven judges, three of whom must reside in the Washington, D.C. area.

Procedural Changes: None are required.

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

5. Changes in FISA Pen Register/Trap and Trace Authority

Section 214 makes a substantial revision to the standard for a FISA pen register/trap and trace. Prior to the Act, FISA pen registers required two showings: (1) relevance to an investigation, and (2) specific and articulable facts giving reason to believe that the targeted line was being used by an agent of a foreign power, or was in communications with such an agent, under specified circumstances. Section 214 simply eliminates the second of the required showings. FISA pen/trap and trace orders are now available whenever the FBI certifies that "the information likely to be obtained is foreign intelligence information not concerning a United States person, or is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution." b1 b5

This new standard requires that the information sought be relevant to an "ongoing investigation to protect against international terrorism or clandestine intelligence activities." Use of this technique is authorized

[redacted] (S)

Although the language differs somewhat from that used in the previous versions of the statute, [redacted] b5

The Section also inserts the language "provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment of the Constitution of the United States." Congress inserted this to indicate that the technique will not be used against U.S. persons who are merely exercising constitutionally protected rights. [redacted] b5

[redacted] b5

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5

[redacted] For example, information concerning apparent associates or, or individuals in contact with, the subject of a investigation, may be relevant.

Procedural Changes: None are required. The field may continue to request FISA pen register/trap and trace authority through FBIHQ in the established manner. However, the requests now need only contain a brief statement explaining the nature of the investigation and the relevance to that investigation of the information sought through the pen register. NSLU and OIPR will develop additional guidance streamlining the process for requesting this authority.

6. Changes in FISA Business Records Authority

Section 215 changes the business records authority found in Title V of FISA. The old language allowed the FISA Court to issue an order compelling the production of certain defined categories of business records (the records of common carriers, public accommodations, vehicle rentals, and storage facilities) upon a showing of relevance and "specific and articulable facts" giving reason to believe that the person to whom the records related was an agent of a foreign power. Section 215 changes this standard to simple relevance (just as in the FISA pen register standard described above) and gives the Court the authority to compel production of "any tangible things (including books, records, papers, documents, and other items for an investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution." This is the same standard described above for Section 214.

In the past, the FBI has encountered situations in which the holders of relevant records refused to produce them absent a subpoena or other compelling authority. When those records did not fit within the defined categories for National Security Letters or the four categories then defined in the FISA business records section, the FBI had no means of compelling production. With the new language the FBI can seek a FISA court order for any such materials.

Procedural Changes: None are required. The field may continue to request business records orders through FBIHQ in the established manner. However, such requests may now seek production of any relevant information, and need only contain information establishing such relevance. NSLU and OIPR will develop additional guidance streamlining the process for requesting this authority.

7. Changes to "Primary Purpose" Standard in FISA

Sections 218 and 504 clarify the "primary purpose" issue in the FISA statute. In its prior form, the FISA required a certification that foreign intelligence be "the" purpose of the requested authority. The FISA Court interpreted this to mean that foreign intelligence, as opposed to criminal prosecution, had to be the "primary"

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

purpose of the requested authority. Thus, interaction between FBI personnel involved in a FISA and criminal prosecutors could call into question the primary intelligence purpose of the FISA (by indicating a purpose different from foreign intelligence). As a result, FISA pleadings have often contained detailed accounts of all communication with criminal prosecutors in cases involving FISA.

Section 218 changes FISA to require a certification that foreign intelligence be "a significant purpose" of the authority sought. Section 504 amends FISA to allow that personnel involved in a FISA may consult with law enforcement officials to coordinate efforts to investigate or protect against attacks, terrorism, sabotage, or clandestine intelligence activities, and that such consultation does not, in itself, undermine the required certification of "significant purpose."

These changes are meant to allow FBI agents greater latitude to consult criminal investigators or prosecutors without putting their FISAs at risk. As such, these changes address extraordinarily complex issues that have long occupied the FISA Court and DOJ. FBIHQ expects that DOJ shortly will issue revised policy on these topics.

Procedural Changes: None are required at present. The field should be aware that greater consultation with prosecutors is now possible, but, given the continuing uncertainty surrounding these issues, should continue to coordinate such consultation through FBIHQ. Additional guidance will be issued.

8. Civil Liability for Unauthorized Disclosure

Section 223 establishes civil liability for certain unauthorized disclosures, including unauthorized disclosures of FISA information. In reference to FISA, this is simply an expansion of existing civil liability, and should not significantly affect operations (since unauthorized disclosure of FISA information is already subject to more severe criminal penalties).

Procedural Changes: None are required. OGC may issue a more detailed analysis of this provision at a later date.

9. Immunity for Compliance with FISA

Section 225 grants providers of wire or electronic communication service, landlords, custodians, and other persons with immunity from civil liability for complying with the requirements of FISA. This provision simply clarifies that persons assisting the FBI in the execution of a FISA order are not at risk of civil lawsuits.

Procedural Changes: None are required.

10. Disclosure of Foreign Intelligence Information to the DCI

Section 905 establishes an affirmative requirement, subject to certain exceptions, that federal law enforcement components must expeditiously disclose to the Director of Central Intelligence any foreign intelligence acquired in the course of criminal investigations. The Attorney General will, within the next six months, develop guidelines to govern such disclosures.

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

To: All Divisions From: Office of the General Counsel
Re: 66F-HQ-A1247863, 10/26/2001

LEAD(s):

Set Lead 1: (Adm)

ALL RECEIVING OFFICES

Disseminate to personnel involved in FCI/IT operations and to other division personnel as appropriate.

♦♦

b6
b7C

From: [redacted]
Sent: Monday, February 09, 2004 10:55 AM
To: [redacted]
Cc:
Subject: RE: TTIC

Federal Tax Records

The FBI is authorized to receive federal tax returns and return information, pursuant to 26 USC §6103(i), upon grant of ex parte order by Federal District Court Judge, or upon written request signed by the Director, FBI (for limited information- not returns). [redacted]

[redacted] b5

[redacted] b5

Title III Derived Information

18 USC 2517(6) allows "foreign intelligence" "counterintelligence" or "foreign intelligence information" obtained via a Title III intercept to be disclosed to any Federal law enforcement or intelligence official (among others) to assist in the performance of his duties. [redacted] b5

[redacted] The Attorney General Guidelines for disclosure of this information (implementation of Patriot Act Sections 203 and 905(a)) require that the prosecuting official be consulted prior to disclosure (except for threat information), and that information identifying US Persons be so marked. Use restrictions may be added if deemed necessary.

Medical Records

The Medical Records Privacy Regulations issued pursuant to HIPAA do not regulate the FBI's handling or disclosure of medical records, they only apply to health care providers, health plans (insurance companies) and health care clearinghouses (billing companies).

Protected health information (a patient's medical records) ~~obtained by the FBI during a health care~~ fraud investigation may not be used for unrelated civil, administrative, or criminal investigations of a

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

non-health oversight matter, except when the balance of relevant factors weighs clearly in favor of its use (as determined by the DAG, DOJ), pursuant to Executive Order 13181 (Dec. 20, 2000). In addition, medical records obtained with an administrative subpoena pursuant to 18 USC 3486 (health care fraud cases) may not be used against the individual in an unrelated administrative, civil or criminal action or investigation, without a court order. [redacted] b5

[redacted]

Drug and alcohol abuse records can only be obtained by the FBI with the patient's consent, or with a court order. If the FBI obtained the records with the patient's consent, the FBI must also have the patient's consent to authorize any redisclosure. 42 CFR 2.32. If a court order was used, further disclosure by the FBI is governed by the terms of that court order. 42 USC §290dd-2(b)(2)(C). Without such explicit authorization, no drug/alcohol abuse records may be disclosed to TTIC.

[redacted] b5

-----Original Message-----
From: [redacted] b6
Sent: Monday, February 02, 2004 4:12 PM b7C
To: [redacted] b5
Cc: b6
Subject: TTIC b7C

[redacted]

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

11 April 2002. Thanks to Declan McCullagh.
Source: http://www.politechbot.com/docs/ashcroft.info.sharing.041102.pdf (215KB)

See DoJ press release:

http://www.usdoj.gov/opa/pr/2002/April/02_ag_211.htm

[5 pages.]

Office of the Attorney General

Washington, D.C. 20530

April 11, 2002

MEMORANDUM FOR THE DEPUTY ATTORNEY GENERAL, THE ASSISTANT ATTORNEY GENERAL FOR THE CRIMINAL DIVISION, THE ASSISTANT ATTORNEY GENERAL FOR LEGAL POLICY, THE DIRECTOR OF THE FEDERAL BUREAU OF INVESTIGATION, THE COMMISSIONER OF THE IMMIGRATION AND NATURALIZATION SERVICE, THE ADMINISTRATOR OF THE DRUG ENFORCEMENT ADMINISTRATION, THE DIRECTOR OF THE EXECUTIVE OFFICE OF UNITED STATES ATTORNEYS, THE DIRECTOR OF THE MARSHALS SERVICE, AND THE DIRECTOR OF THE FOREIGN TERRORIST TRACKING TASK FORCE.

FROM: THE ATTORNEY GENERAL *[Signed]*

SUBJECT: Coordination of Information Relating to Terrorism

The prevention of terrorist activity is the overriding priority of the Department of Justice. By memoranda dated November 8 and 13, 2001, I directed Department components to review their policies and procedures to ensure information sharing, information analysis, and coordination of activities with federal, state and local agencies to prevent acts threatening public safety and national security. The Deputy Attorney General has reported to me the specific actions taken to implement those directives. I commend you on the substantial progress the Department has achieved in analyzing information, sharing intelligence and coordinating activities in the multi-front effort to combat terrorism.

I am hereby directing you to undertake further action to institutionalize the Department's ongoing efforts to coordinate information and activities to prevent and disrupt terrorist activities.

1. Expand Terrorist Information in Law Enforcement Databases.

The Federal Government maintains a number of databases that provide real-time information to officials in foreign diplomatic outposts, at border points of entry, and for interior domestic law enforcement. Expansion of information in such databases relating to known and suspected terrorists will greatly enhance the ability of federal, state, and local officials to prevent terrorists from obtaining visas to enter the United States, to deny them entry into our borders, to detect and apprehend those already in the country, and to gather intelligence on the plans and activities of terrorist conspiracies. Accordingly, I hereby direct all investigative components within the Department of Justice to establish procedures to

provide, on a regular basis and in electronic format, the names, photographs (if available), and other identifying data of all known or suspected terrorists for inclusion in the following databases:

- The Department of State TIPOFF System. This system is designed to detect known or suspected terrorists who are not U.S. citizens as they apply for visas overseas or as they attempt to pass through U.S., Canadian, and Australian border entry points. Expanding terrorist information in the database will preclude the issuance of visas to known terrorists; warn U. S. diplomatic posts of the security risk posed by certain applicants; and alert intelligence and law enforcement agencies of the travel plans of suspected terrorists.

- The FBI National Crime Information Center (NCIC). The NCIC is the nation's principal law enforcement automated information sharing tool. It provides on-the-street access to information to over 650,000 U.S. local, state, and federal law enforcement officers. The inclusion of terrorist information in this powerful database will assist in locating known foreign terrorists who have entered the U.S. undetected, warn law enforcement officers of a potential security risk, and alert intelligence and law enforcement agencies of the presence of a suspected terrorist at a specific location and time. Agencies contributing terrorist information should establish procedures and protocols for direct electronic input of the data into NCIC, observing applicable restrictions on the entry of classified information into the system. To expand further local and state law enforcement access to relevant terrorist information, the FBI shall establish procedures with the Department of that that will enable, on a recurring basis, the inclusion of qualifying TIPOFF data into NCIC. The FBI shall establish procedures that inform law enforcement officers what action should be taken when encountering suspected terrorists. Furthermore, the NCIC must properly characterize individuals as either suspected terrorists or known terrorists, with the latter designation reserved for individuals against whom sufficient evidence exists to justify such a determination.

- The U.S. Customs Service Interagency Border Inspection System (IBIS). This system is the primary automated screening tool used by both the Immigration and Naturalization Service (INS) and U.S. Customs Service at ports-of-entry. The inclusion of terrorist data in this integrated database will help preclude the entry of known and, suspected terrorists into the U.S., warn inspectors of a potential security threat, and alert intelligence and law enforcement agencies that a suspected terrorist is attempting to enter the U.S. at a specific location and time. Such information on known or suspected foreign terrorists must be placed in IBIS unless it is already accessible through an automated IBIS query of NCIC.

The procedures established for providing information to the databases listed above may allow for case-by-case exceptions where the component head or his responsible designee determines that disclosure would compromise classified information, jeopardize an investigation, or compromise a confidential source.

2. Coordinate Foreign Terrorist Information.

The international response to the September 11th attacks has been defined by multilateral cooperation and resolve to restore security and liberty to freedom-loving people of the world. The success of the response has depended in large part on improved sharing among governments of information relating to terrorists, their associates, and their activities. Continued vigilance against international terrorist conspiracies requires procedures to institutionalize such information coordination. Accordingly, I hereby direct the FBI, through its Legal Attaches, to establish procedures to obtain on a regular basis the fingerprints, other identifying information, and available biographical data of all known or suspected foreign terrorists who have been identified and processed by foreign law enforcement agencies. The FBI shall also coordinate with the Department of Defense to obtain, to the extent permitted by law, on a

regular basis the fingerprints, other identifying information, and available biographical data of known or suspected foreign terrorists who have been processed by the U.S. Military. Such information shall be placed into the Integrated Automated Fingerprint Identification System (IAFIS) and other appropriate law enforcement databases to assist in detecting and locating foreign terrorists.

3. Establish Secure System for Information Coordination with State and Local Partners.

The various information systems described above are databases, triggered by a name query, that serve as an alert mechanism and pointer index. Effective information coordination requires more sophisticated mechanisms for expanded searches, multipoint information flow, and integrated analysis. Federal agencies have the benefit of classified systems that enable keyword searches of relevant documents, secure e-mail, and other important collaborative information sharing tools, However, there is no corresponding national system with comparable capability for integrated information coordination on counterterrorism with and among state and local law enforcement agencies.

By memorandum of November 13, 2001, I directed all U.S. Attorneys to develop protocols for coordinating information to, from, and among our state and local par in law enforcement. I encouraged the use, where practicable, of technologies already available and currently in use by the Department to facilitate information-sharing. I hereby direct the Deputy Attorney General to coordinate among the applicable components the development of a secure but unclassified web-based system to enable local, state, and federal users to post, retrieve, and read information, restrict access to certain products, send secure e-mail, and receive automatic e-mail notifications when new items are posted. This integrated system should allow for future capabilities, such as imagery and photographs, instant messaging and database access and restricted access to classified information at least at the Secret level and ideally in higher classifications.

4. Analyze Foreign Terrorist Data.

On October 30, 2001, the President directed that the Department establish the Foreign Terrorist Tracking Task Force (FTTTF). The mission of the FTTTF is to keep foreign terrorists and their supporters out of the United States by providing critical and timely information to border control and interior enforcement agencies and officials. To do so requires electronic access to large sets of data, including the most sensitive material from law enforcement and intelligence sources. Analyzing such data will enable the FTTTF to discern patterns and probabilities of terrorist activities.

I hereby direct the FTTTF to identify the agency information systems and data sets needed to fulfill its mission. Each agency is to provide to the FTTTF unfiltered, timely and electronic access to the information systems and data sets deemed relevant by the Director of the FTTTF, subject to any legal restrictions on the sharing of such information.

5. Standardize Procedures for Sharing of Sensitive Information.

Section 203 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. 107-56, authorizes the sharing of foreign intelligence and counterintelligence information obtained as part of a criminal investigation, including through grand jury proceedings and Title III electronic surveillance, with relevant Federal officials to assist in the performance of their duties. The officials receiving such information may use it only as necessary in the conduct of their official duties and subject to any limitations on the unauthorized disclosure of such information. The Criminal Division has developed and distributed model forms to be used to notify the supervising court when grand jury information has been shared

pursuant to section 203.

Section 905 of the USA PATRIOT Act requires the Department and other Federal agencies with law enforcement responsibilities to share expeditiously foreign intelligence obtained in the course of a criminal investigation with the Director of Central Intelligence, subject to limitations otherwise provided by law and exceptions delineated in regulations to be issued by the Department. In the types of criminal cases in which foreign intelligence information is commonly encountered -- including terrorism, drug trafficking, and organized crime investigations -- strong relationships for information-sharing and coordination w the Intelligence Community are already in place.

I hereby direct the Assistant Attorney General for Legal Policy, in consultation with the Criminal Division, FBI, and other relevant components, to draft, for my consideration and promulgation, procedures, guidelines, and regulations to implement sections 203 and 905 of the USA PATRIOT Act in a manner that makes consistent and effective the standards for sharing of information, including sensitive or legally restricted information, with other Federal agencies. Those standards should be directed toward, consistent with law, the dissemination of all relevant information to Federal officials who need such information in order to prevent and disrupt terrorist activity and other activities affecting our national security. At the same time, the procedures, guidelines, and regulations should seek to ensure that shared information is not misused for unauthorized purposes, disclosed to unauthorized personnel, or otherwise handled in a manner that jeopardizes the rights of U.S. persons, and that its use does not unnecessarily affect criminal investigations and prosecutions. The standards adopted will govern the coordination of information directed by this memorandum, and well as other voluntary or mandated sharing of criminal investigative information.

* * *

The September 11 attacks demonstrate that the war on terrorism must be fought and won at home as well as abroad. To meet this continuing threat, law enforcement officials at all levels of government -- federal, state, and local -- must work together, coordinating information and leveraging resources in the joint effort to prevent and disrupt terrorist activity. You have worked hard and accomplished much in this common fight, but more remains to be done to help secure America and protect her people. I thank you for your continued service, dedication, and cooperative spirit in this time of continuing national need.

Transcription and HTML by Cryptome.

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 10-05-2005 BY 65179 DMH/JHF 05-CV-0845

ÄÁ□Ø Ø □□ÁTerrorist DNA database

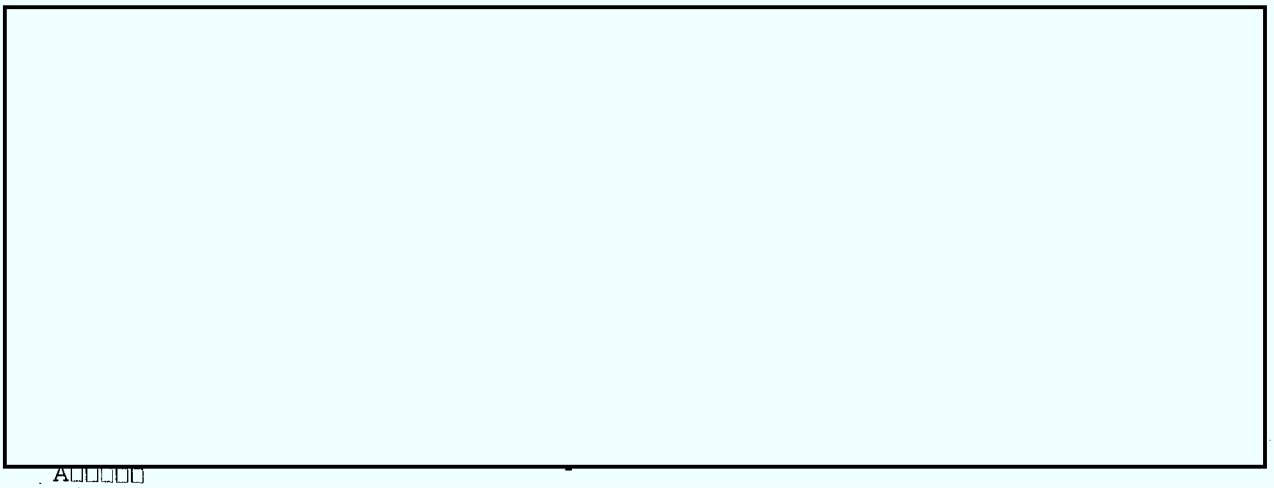
Ð□Ð□□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□°□□□`
□□h□À□□□p□È□ x Ð (#€%Ø'0*^,à.81▯3è5@8~:ð<H? AøCPF¨H□KXM°O□R`T V□Yh[À]
□`□□□□□□□□□□□□□□□□□□□□□□□□°□Ð□□ [redacted]

b5

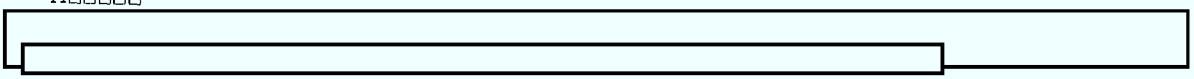
b5
b6
b7C

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5

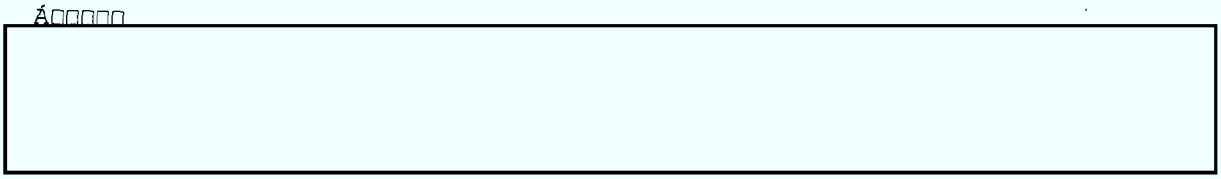


A□□□□□□
□ÁÁ□□□□□
□ÁÁ□□□□□
□ÁÁ□□□□□
□ÁÁ□□□□□
□Á
Á□□□□□



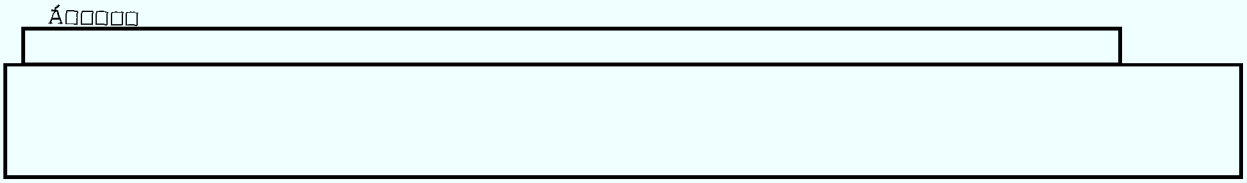
b5

Á□□□□□



b5

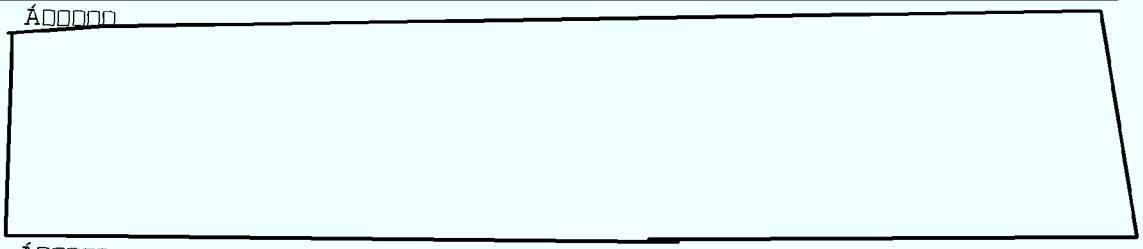
Á□□□□□



b5

b5

Á□□□□□



Á□□□□□

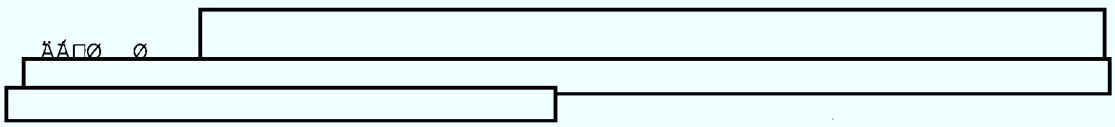
b5

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5
b6
b7C

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

ÃCC:Ä



b6
b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 10-05-2005 BY 65179 DMH/JHF 05-CV-0845

RE sharing DNA profiles with [redacted].txt

From: [redacted] (Div09) (FBI)
Sent: Tuesday, May 04, 2004 6:35 PM
To: [redacted] (LD) (FBI)
Cc:
Subject: RE: sharing DNA profiles with [redacted]

b6
b7C
b7D

UNCLASSIFIED
NON-RECORD

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 10-06-2005 BY 65179 DMH/JHF 05-CV-0845

b2
b5
b6
b7C
b7E

[redacted]

RE sharing DNA profiles with [redacted] txt

[redacted]

b2
b5
b6
b7C
b7E
b7D

Hope this helps--need to run to my bus.....

-----Original Message-----
From: [redacted] (LD) (FBI)
Sent: Tuesday, May 04, 2004 1:25 PM
To: [redacted] (Div09) (FBI)
Subject: FW: sharing DNA profiles with [redacted]

b6
b7C
b7D

UNCLASSIFIED
NON-RECORD

Hi [redacted] -

[redacted]

b2
b6
b7C
b7E

Thanks -
[redacted]

-----Original Message-----
From: [redacted]
Sent: Wednesday, April 07, 2004 1:47 PM
To: [redacted] (Div09) (FBI)
Subject: sharing DNA profiles with [redacted]

b6
b7C
b7D

Expires After: 7/6/2004 00:00

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

RE sharing DNA profiles with [redacted].txt

Hi [redacted]:

Recently I was contacted by [redacted] of CJIS concerning

[redacted]

b2
b5
b6
b7C
b7D
b7E

Thanks, [redacted]

UNCLASSIFIED

UNCLASSIFIED

From: [redacted] (Div09) (FBI)
Sent: Monday, April 19, 2004 9:17 AM
To: [redacted] (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] (Div09) (FBI)
Subject: RE: Restrictions on sharing information with TTIC

b6
b7C

UNCLASSIFIED
NON-RECORD

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 10-06-2005 BY 65179 DMH/JHF 05-CV-0845

[redacted]

b5

-----Original Message-----
From [redacted] (FBI)
Sent: Thursday, March 04, 2004 3:19 PM
To [redacted] (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] (Div09) (FBI)
Subject: Restrictions on sharing information with TTIC

b6
b7C

UNCLASSIFIED
NON-RECORD

Section 203(d) of the Patriot Act provides that "Notwithstanding any other provision of law" it is lawful to share foreign intelligence or counterintelligence (as defined in 50 USC 401a) or foreign intelligence information obtained as part of a criminal investigation with any federal law enforcement, intelligence, protective immigration, national defense, or national security official in order to assist the receiving official in his official duties. The receiving official may use the information only as necessary in the conduct of his official duties subject to any limitation on the unauthorized disclosure of such information.

b5

[redacted]

UNCLASSIFIED

UNCLASSIFIED

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~DATE: 10-06-2005~~
~~CLASSIFIED BY 65179 DMH/SHE 05-CV-0845~~
~~REASON: 1.4 (C , D)~~
~~DECLASSIFY ON: 10-06-2030~~

OGA info REQUIRES CONSULTATION w/OGA per ONSITE LIAISON

From: [redacted] b6
Sent: Tuesday, October 21, 2003 12:47 PM b7C
To: [redacted]
Cc: [redacted] b5 b6 b7C
Subject: SSCRET Material attached RE: Foreign Sharing Authority
SECRET Material attached

[redacted]

-----Original Message-----
From: [redacted]
Sent: Tuesday, October 21, 2003 12:04 PM
To: [redacted]
Subject: FW: Foreign Sharing Authority

DATE: 12-05-2005
CLASSIFIED BY 65179/DMH/LP/DK 05-cv-0845
REASON: 1.4 (C,D)
DECLASSIFY ON: 12-05-2030

b5 b6 b7C

[redacted]

-----Original Message-----
From: [redacted] b6
Sent: Tuesday, October 21, 2003 11:58 AM b7C
To: [redacted] BOWMAN, MARION E.; [redacted]
Cc: [redacted] Briese, M Chris; [redacted]
Subject: RE: Foreign Sharing Authority

[redacted] b5 b6 b7C

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

~~SECRET~~

b6
b7C

Thanks,

[redacted]

-----Original Message-----
From: [redacted] b6
Sent: Tuesday, October 21, 2003 9:54 AM b7C
To: BOWMAN, MARION E.
Cc: [redacted] Briese, M Chris;
Subject: RE: Foreign Sharing Authority

[redacted] b5 b6 b7C

-----Original Message-----
From: [redacted]
Sent: Tuesday, October 21, 2003 8:57 AM
To: BOWMAN, MARION E.;
Cc: [redacted] b6 b7C
Briese, M Chris;
Subject: RE: Foreign Sharing Authority

Spike--

[redacted] b5

[redacted] b1 b5

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b1
b5

[redacted] (S)

-----Original Message-----
From: BOWMAN, MARION E.
Sent: Tuesday, October 21, 2003 5:14 AM
To:
Cc: Briese, M Chris;
Subject: RE: Foreign Sharing Authority

b5
b6
b7C

[redacted]

-----Original Message-----
From:
Sent: Monday, October 20, 2003 5:41 PM
To:
Cc: BOWMAN, MARION E.; Briese, M Chris;
Subject: Foreign Sharing Authority

b6
b7C

[redacted]

b5
b6
b7C
b7D

Thanks,
[redacted]

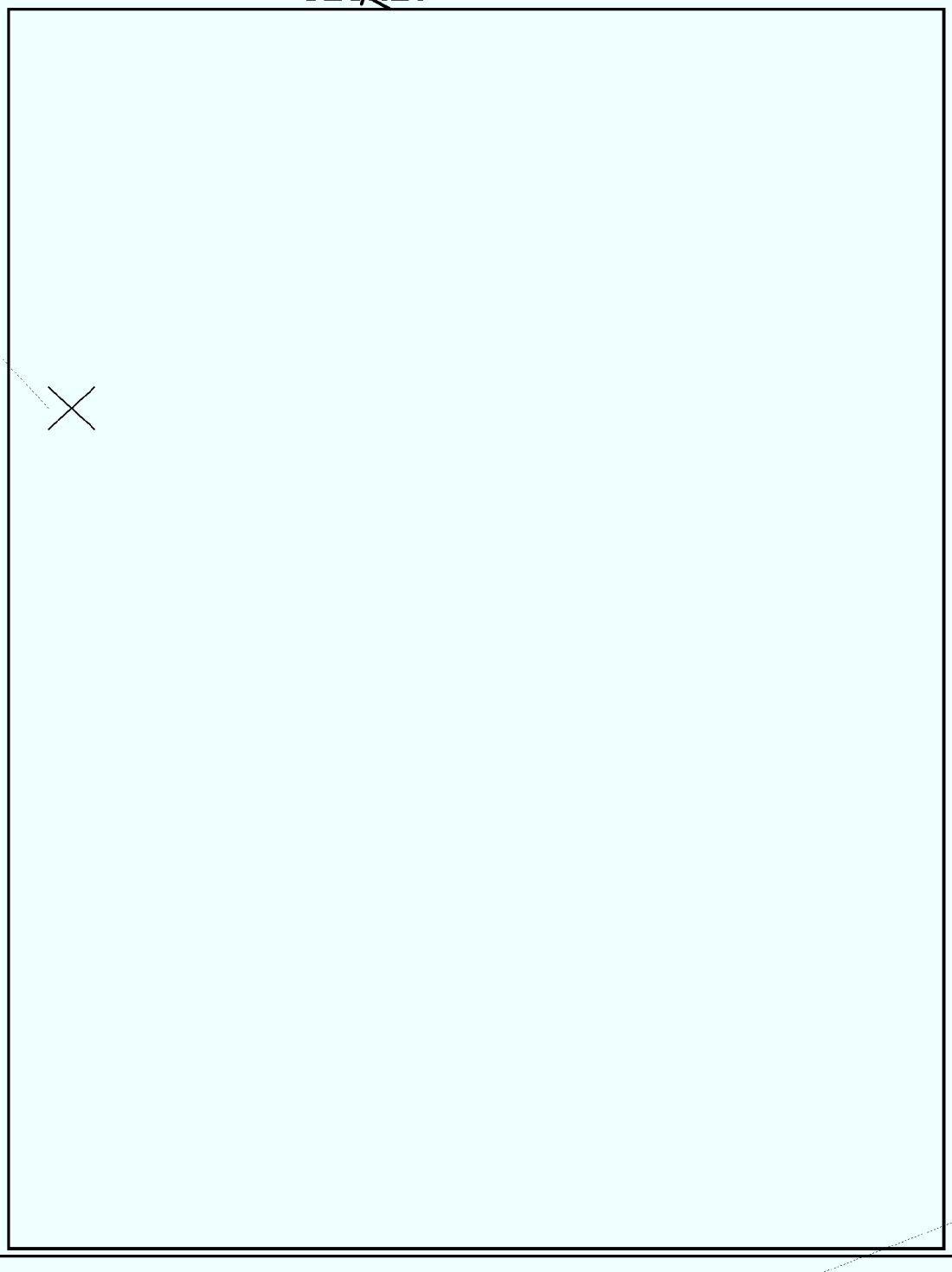
DRAFT 10/20/2003

b5

FBI Authority to Share Information with Foreign Governments

[redacted] (S)

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT



(U)

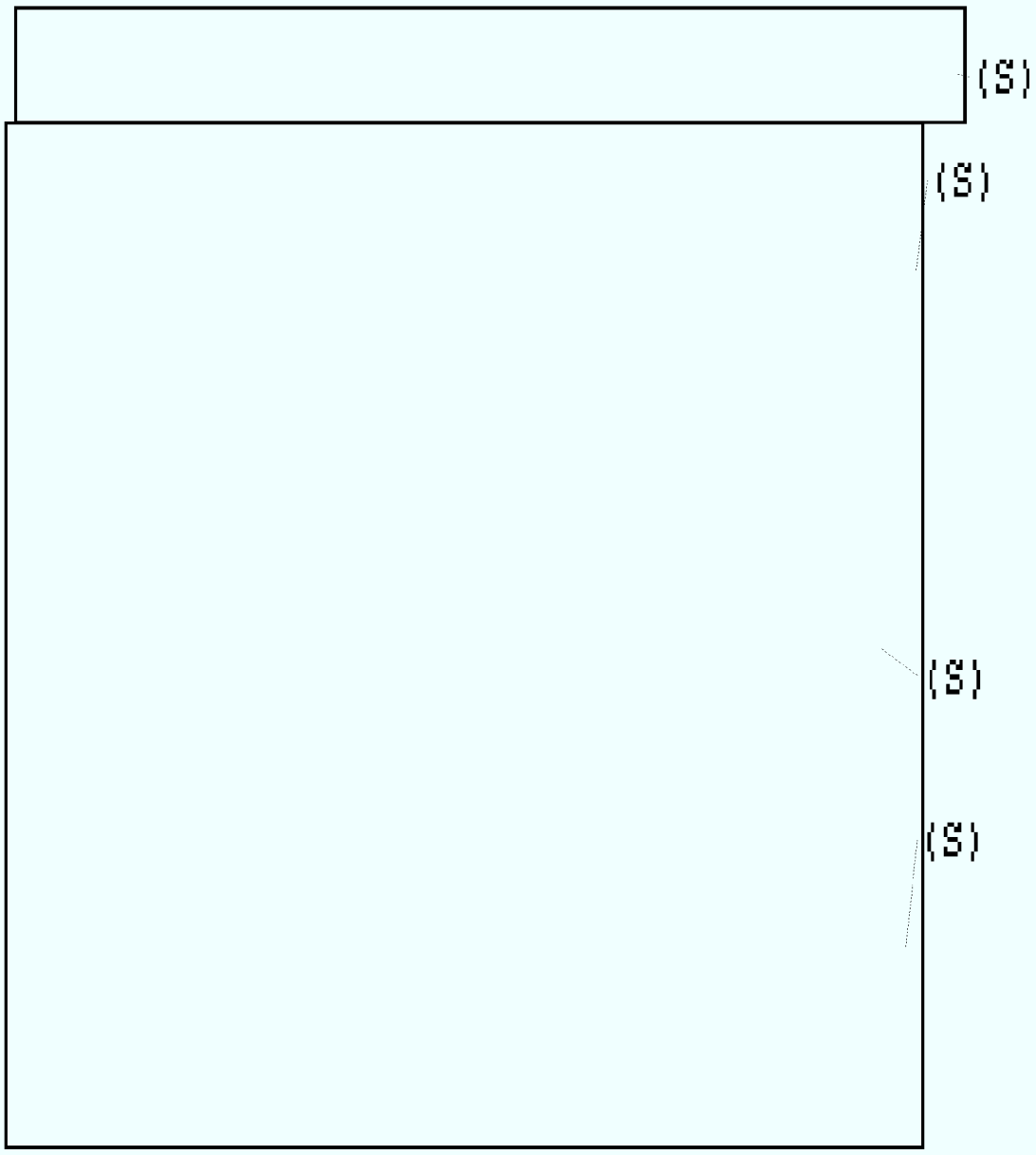
b1
b5

(S)

b1
b5
b2
b7D

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b1
b2
b7D
b5

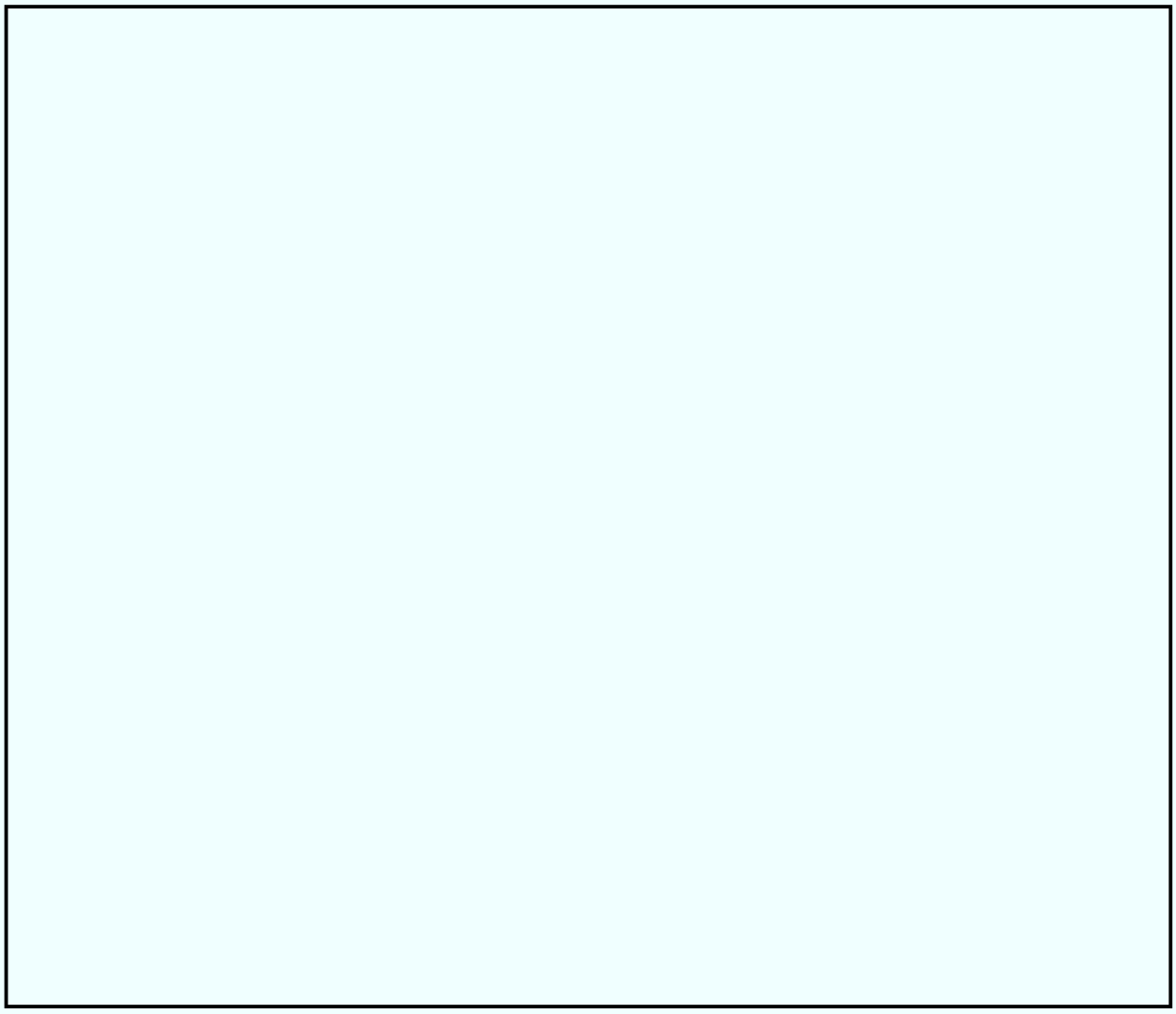


PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

_DRAFT10/14/04

[redacted] b5

[redacted] b5



b5

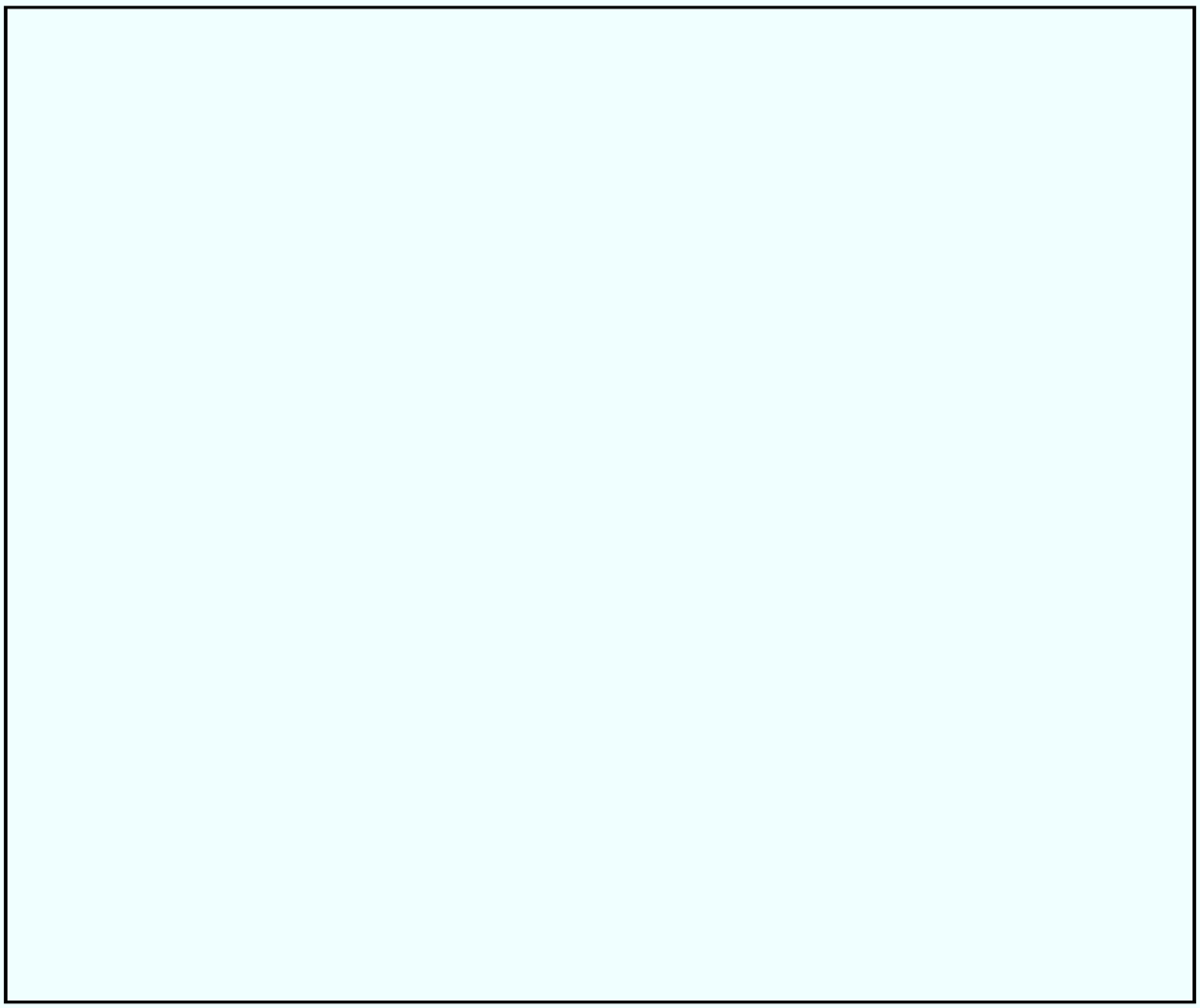
b5

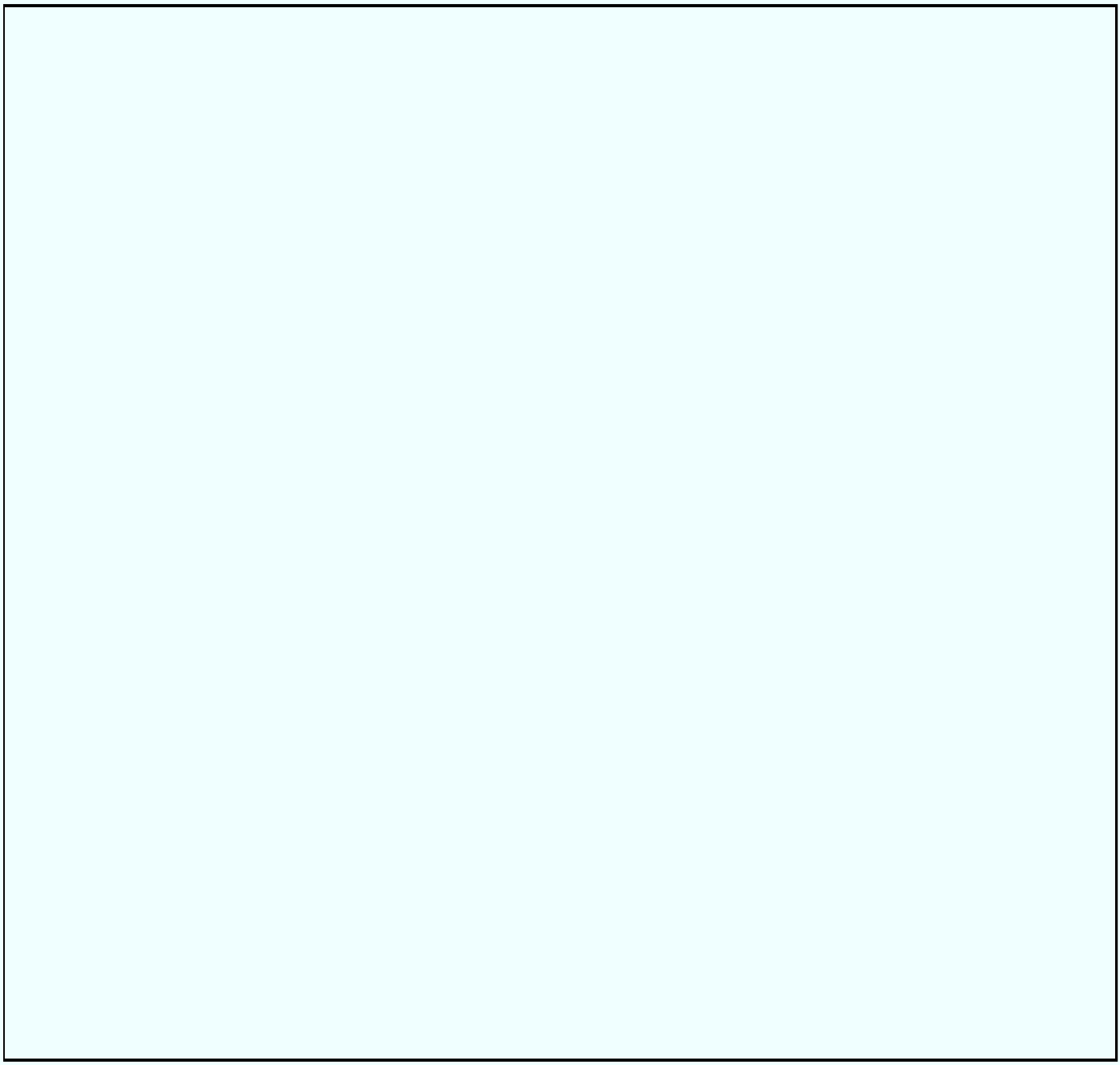
PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

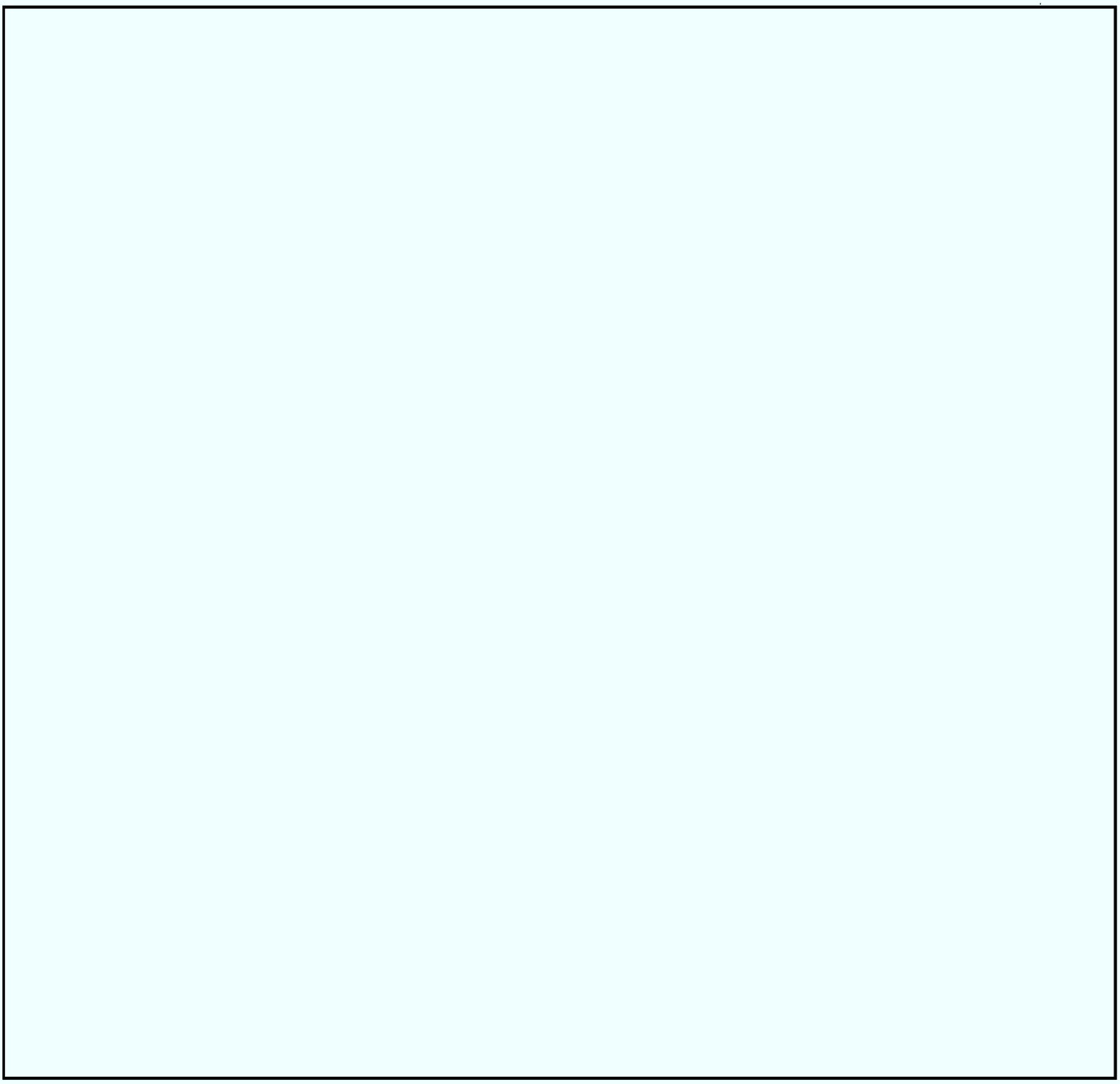
b5

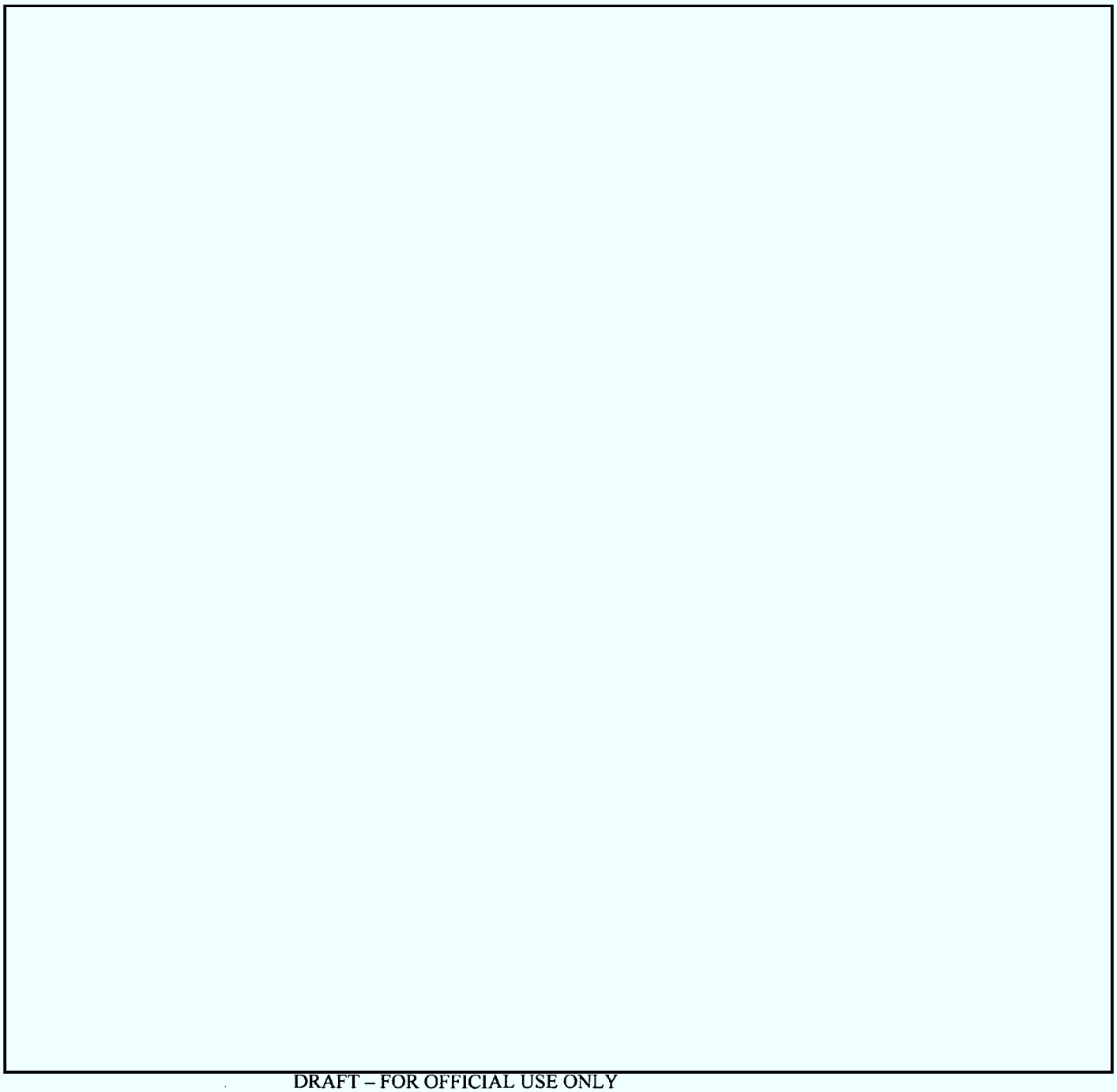
b5

b5

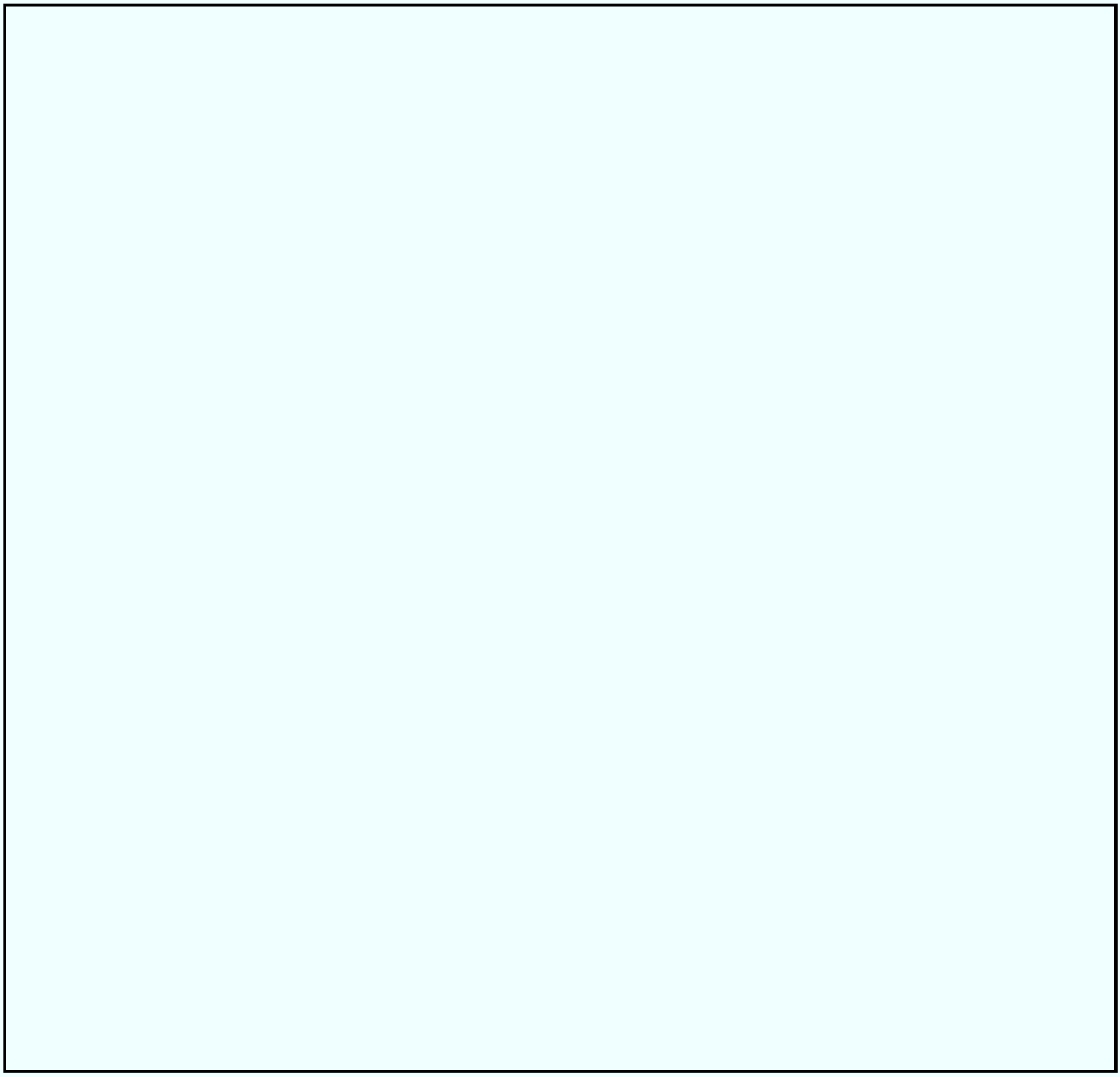




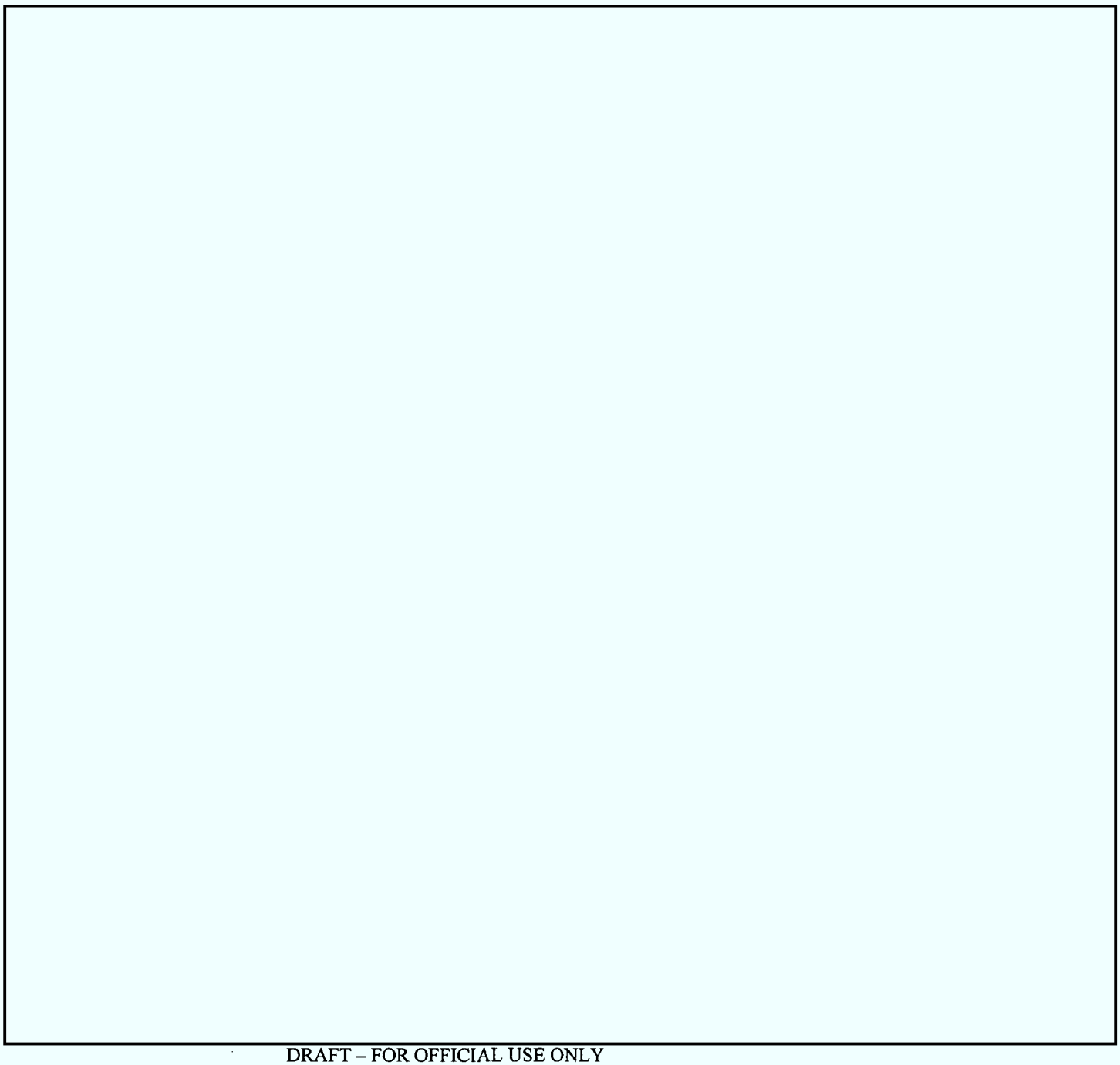




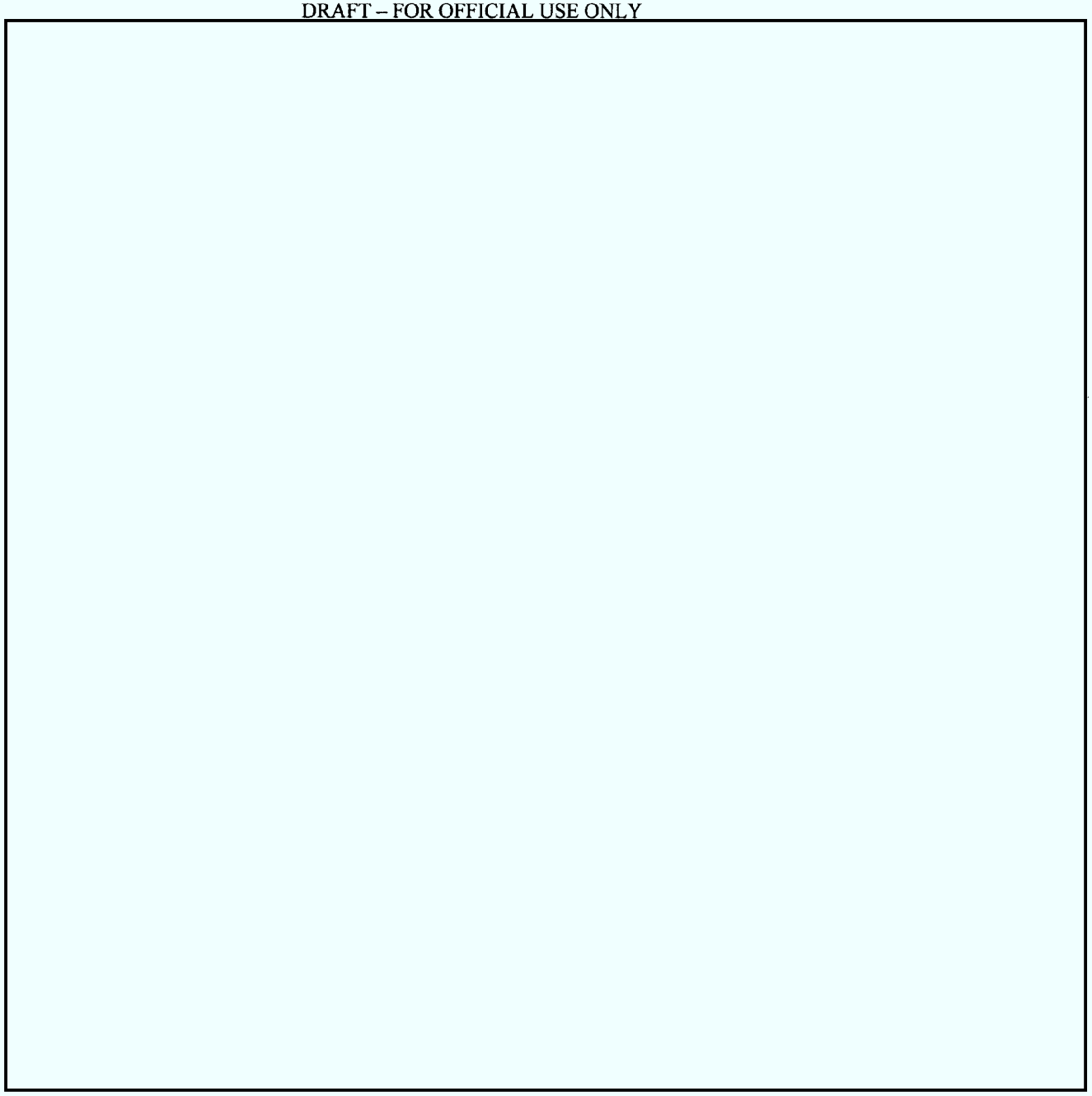
b5



b5



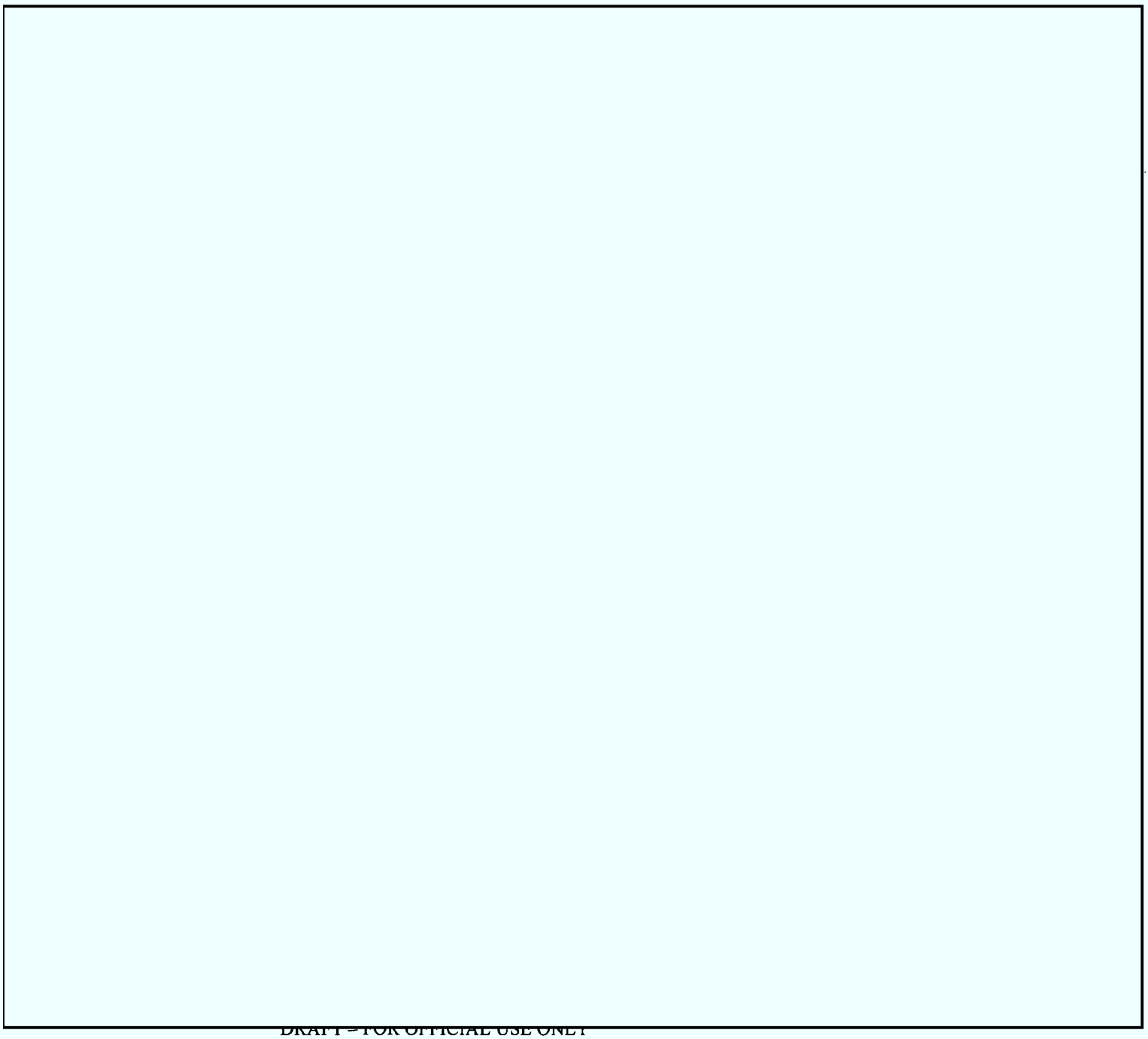
b5



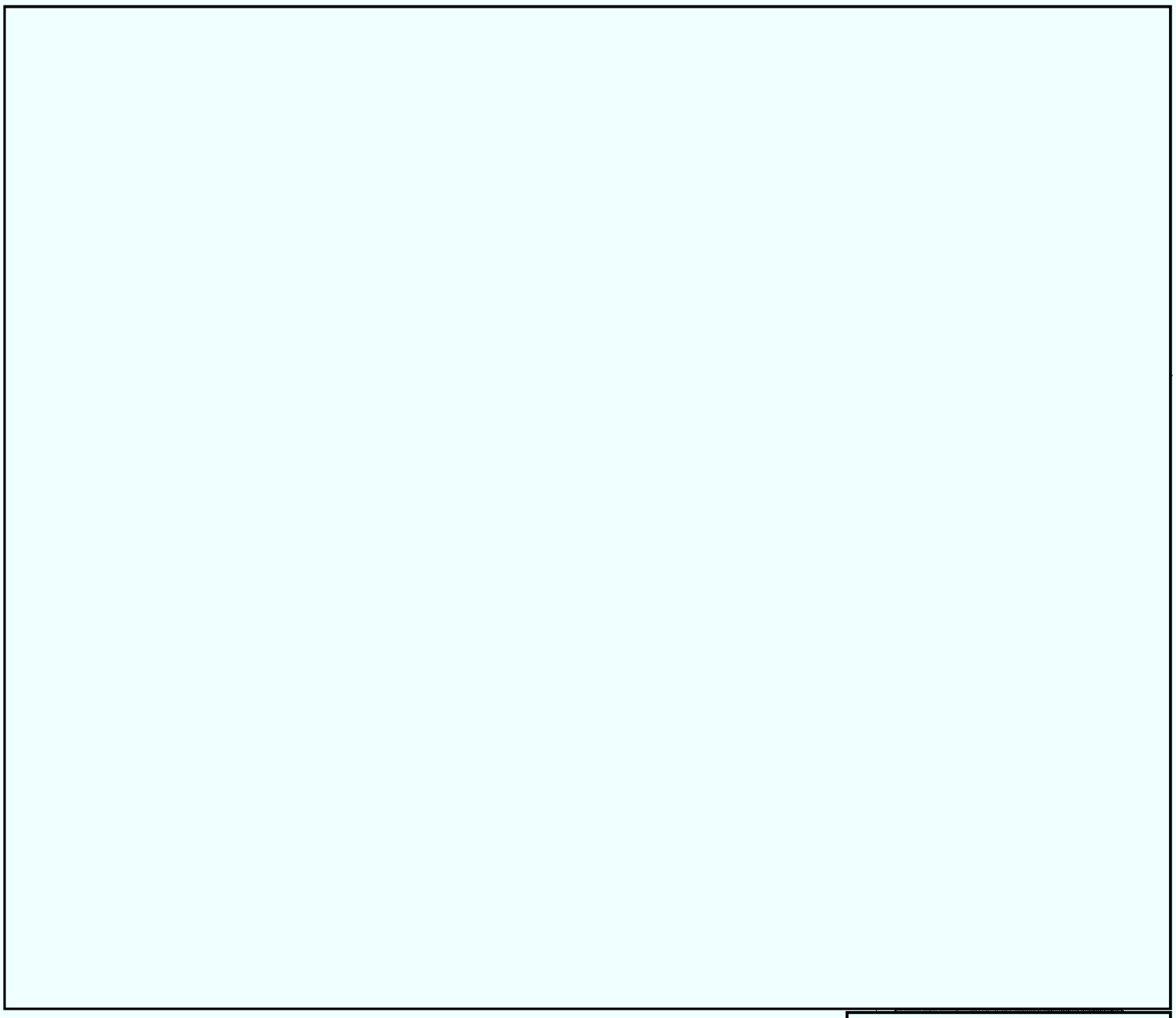
b5

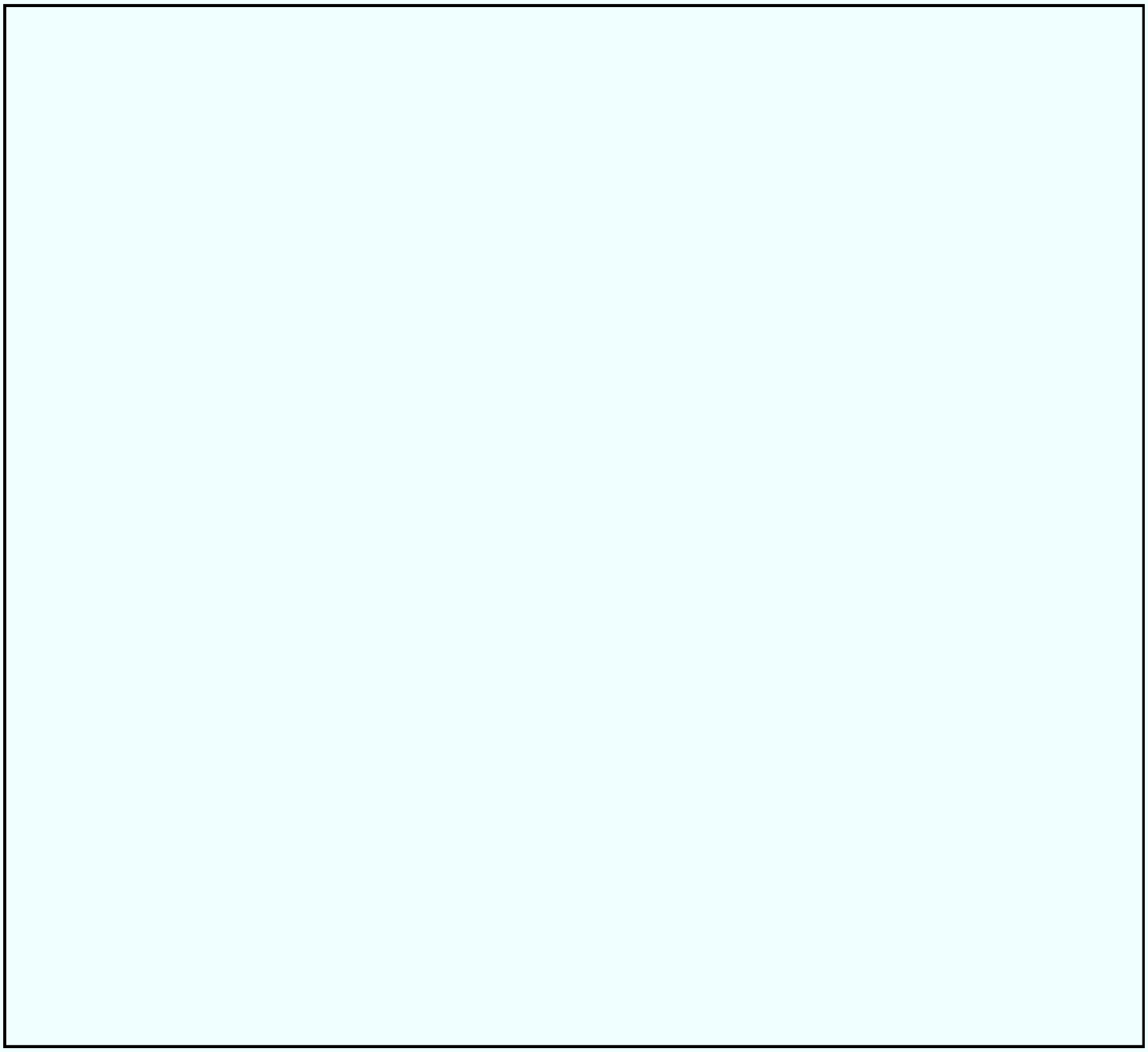
PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5

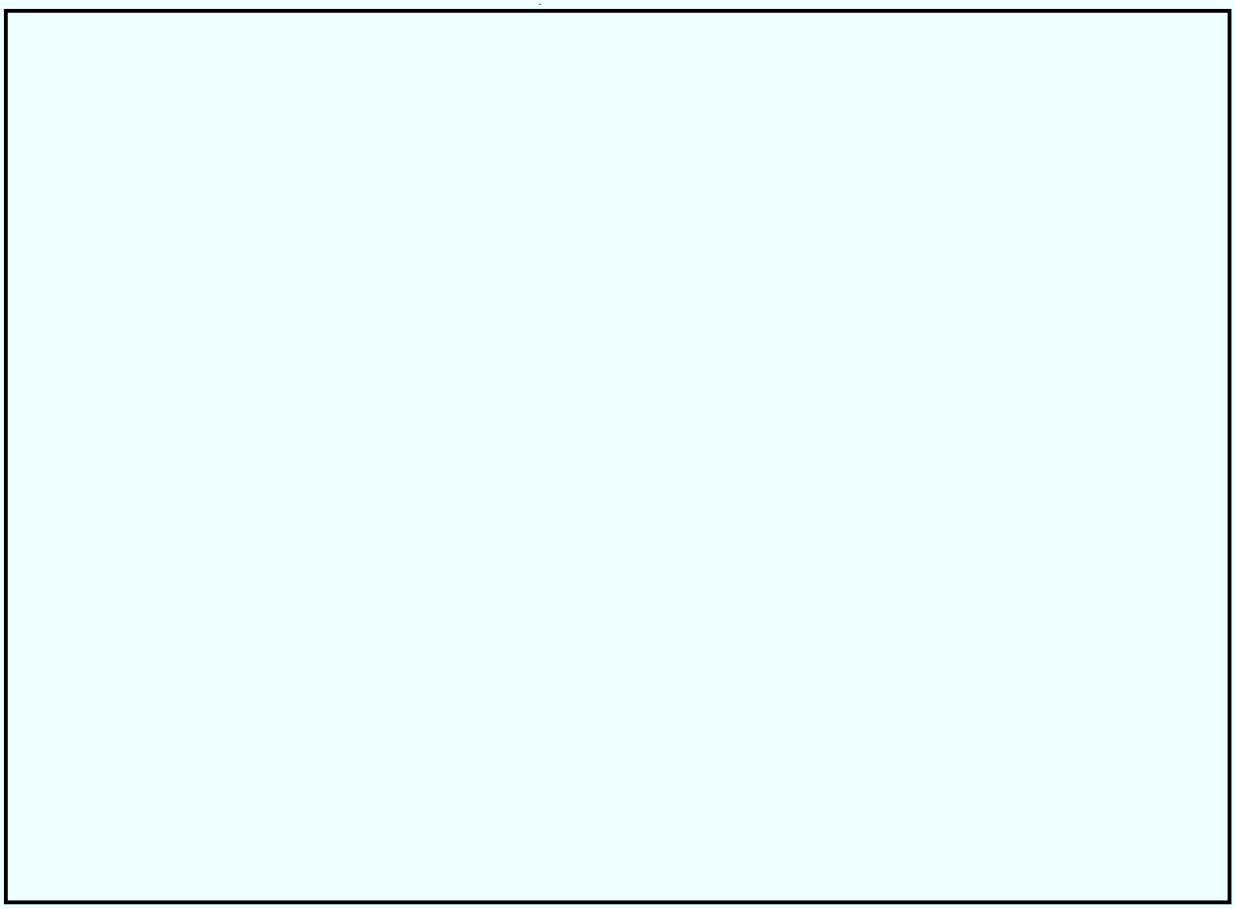


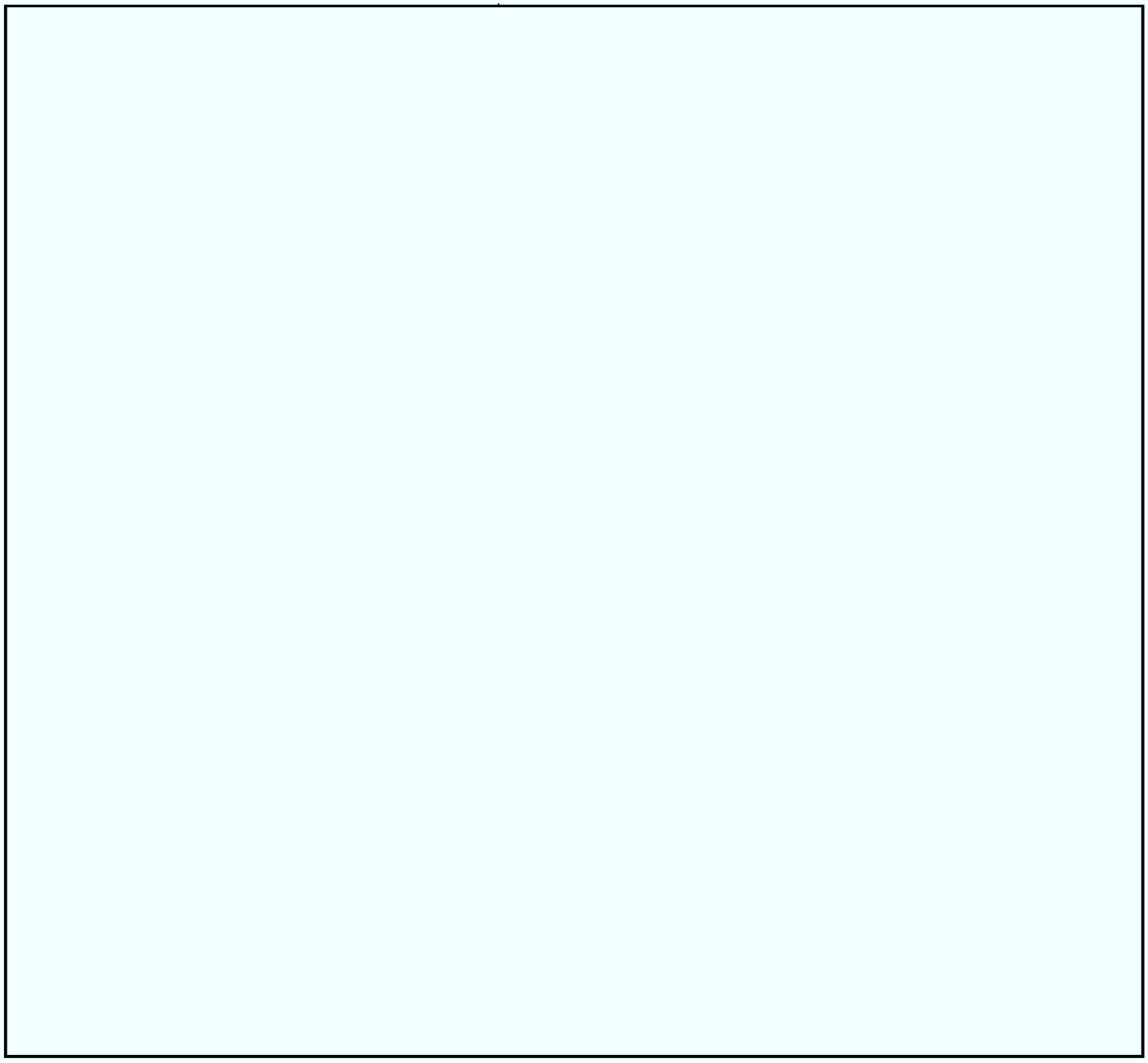
DRAFT – FOR OFFICIAL USE ONLY



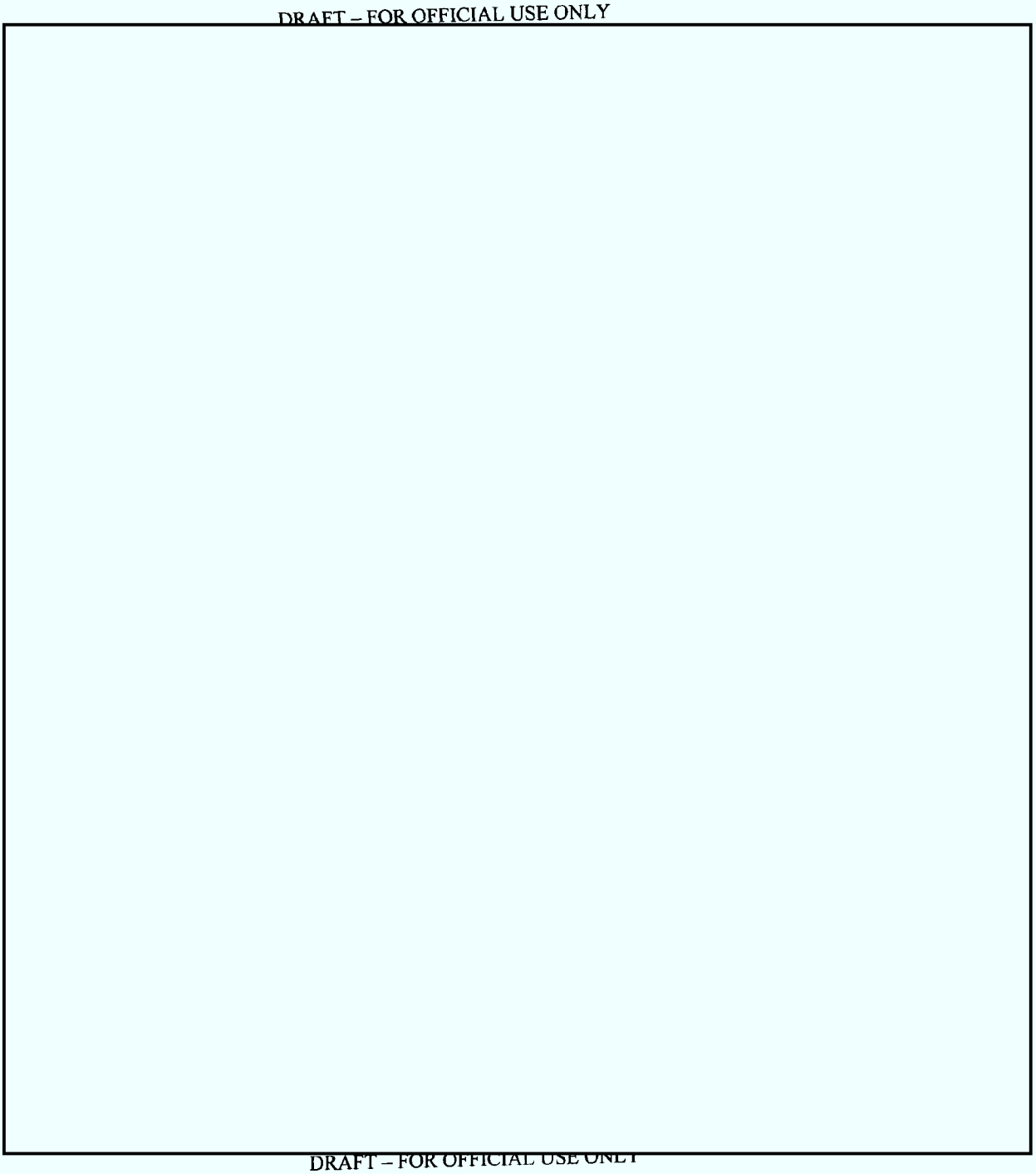


b5

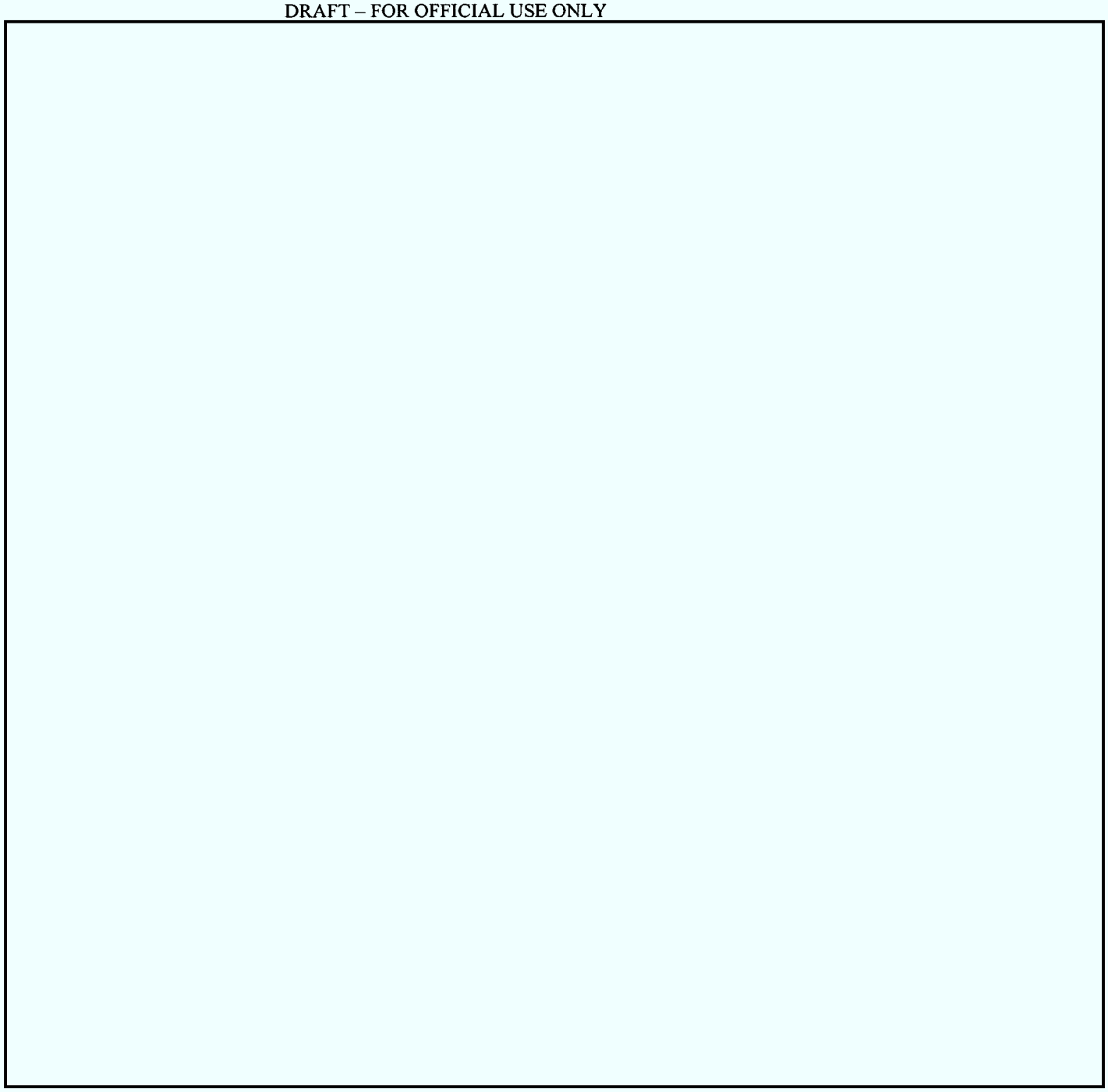




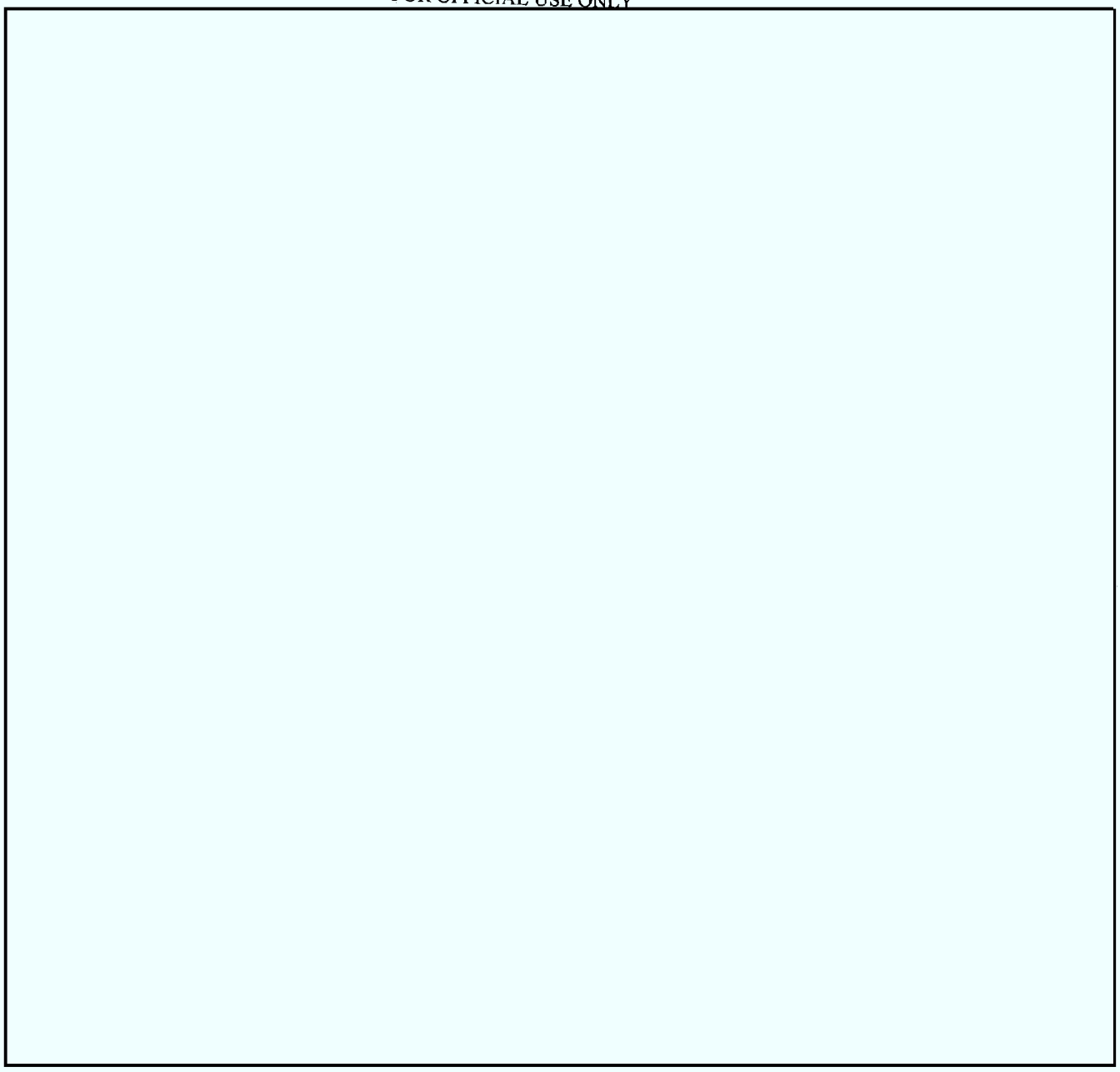
b5

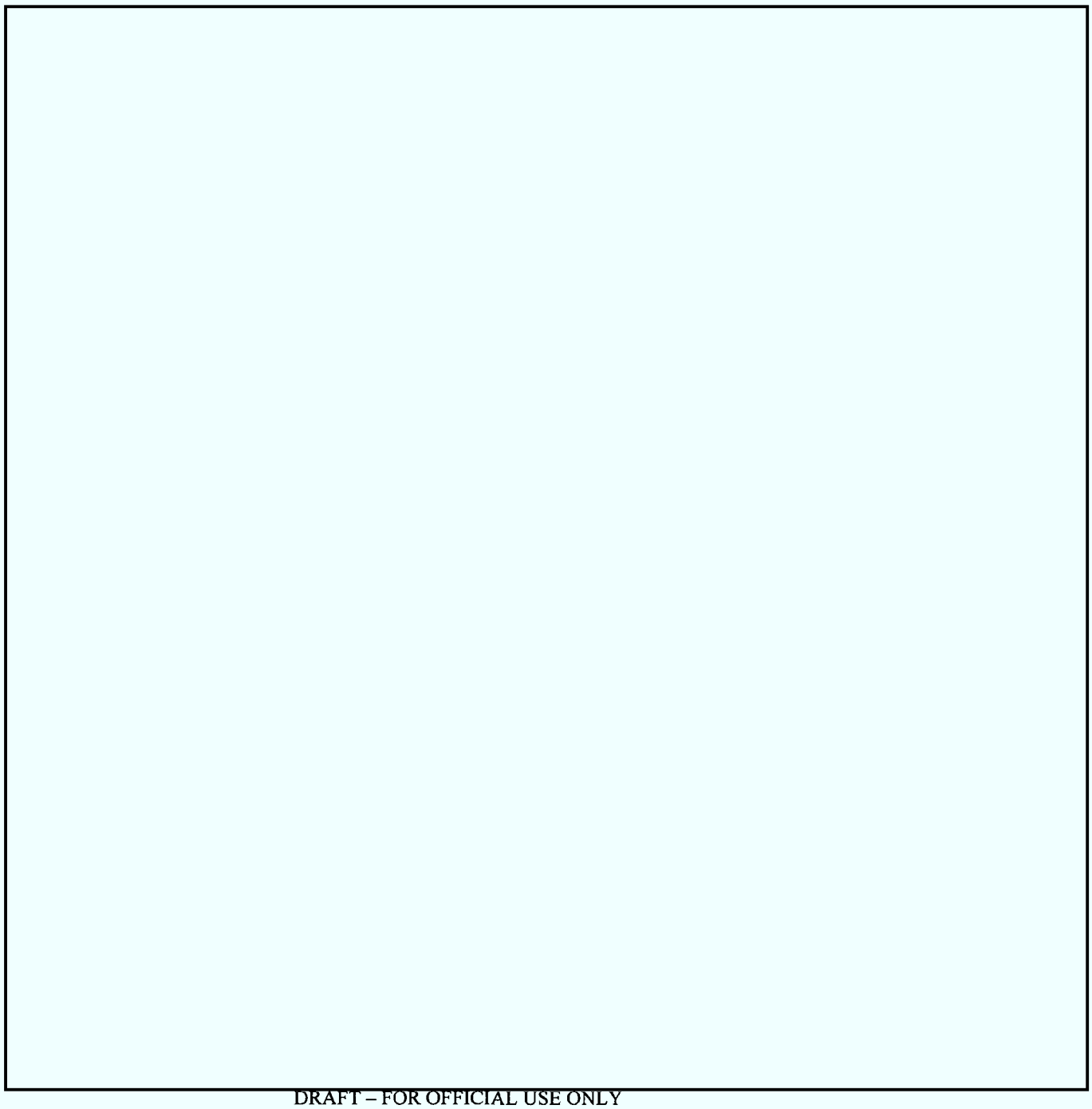


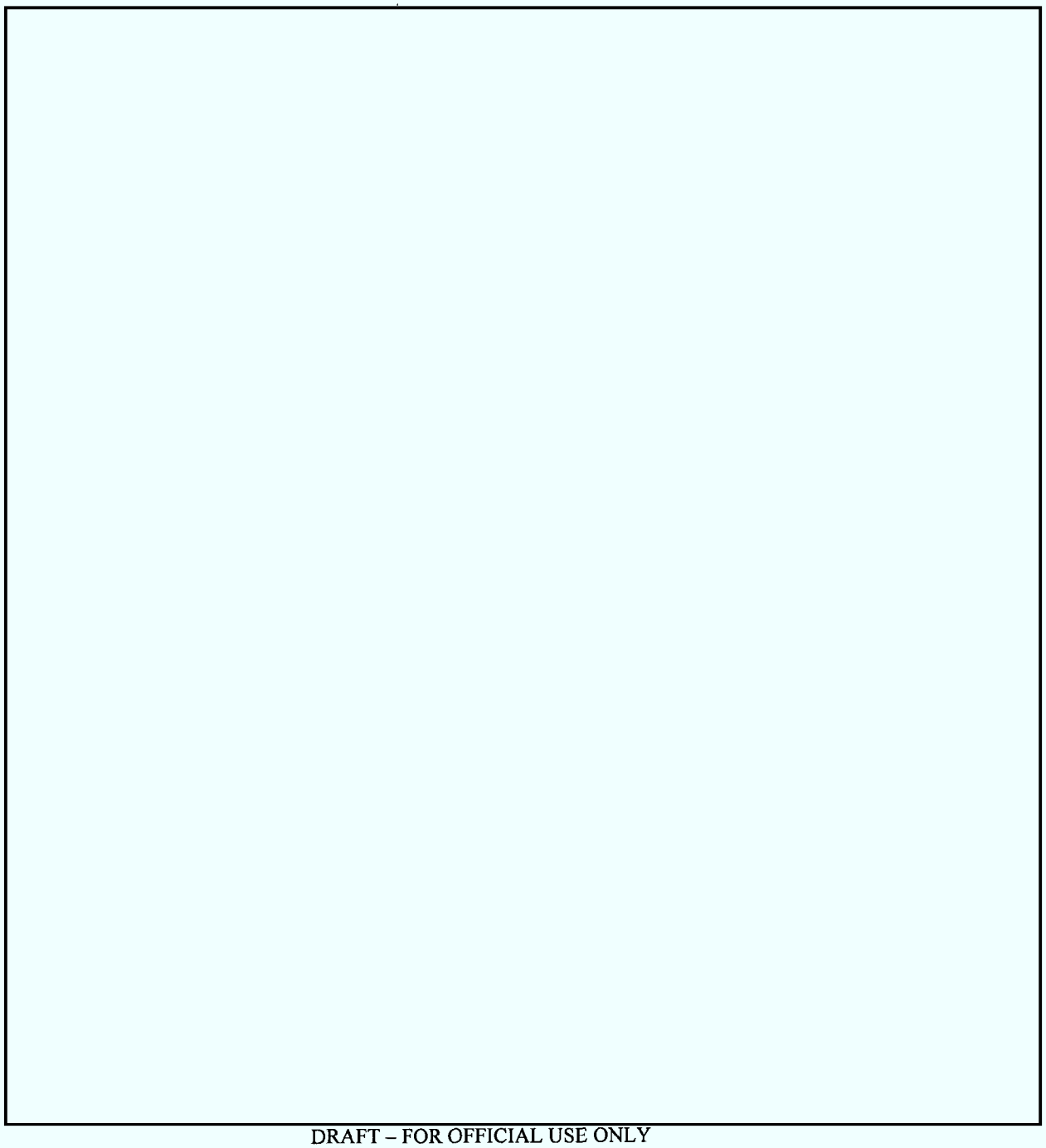
PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT



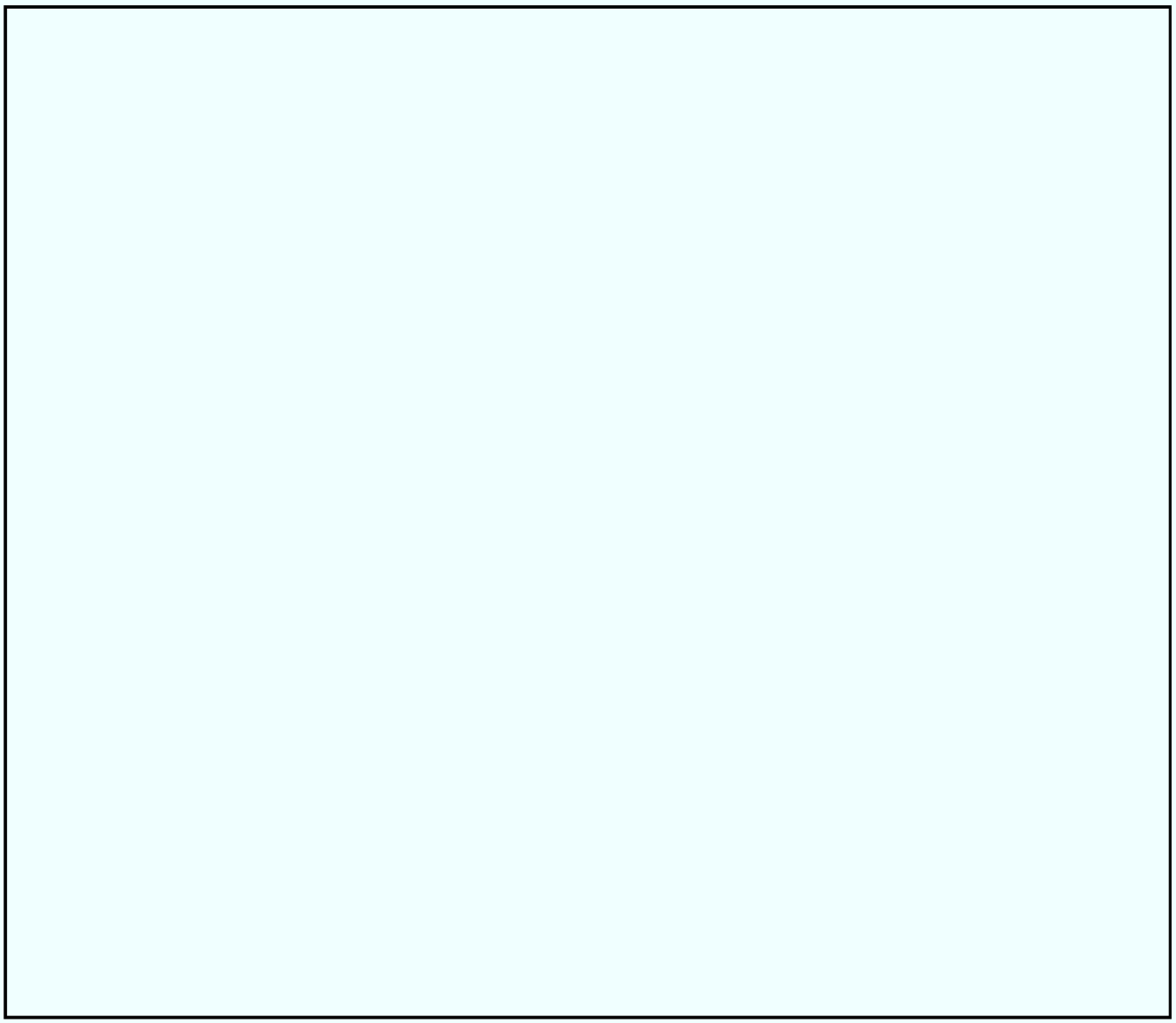
b5



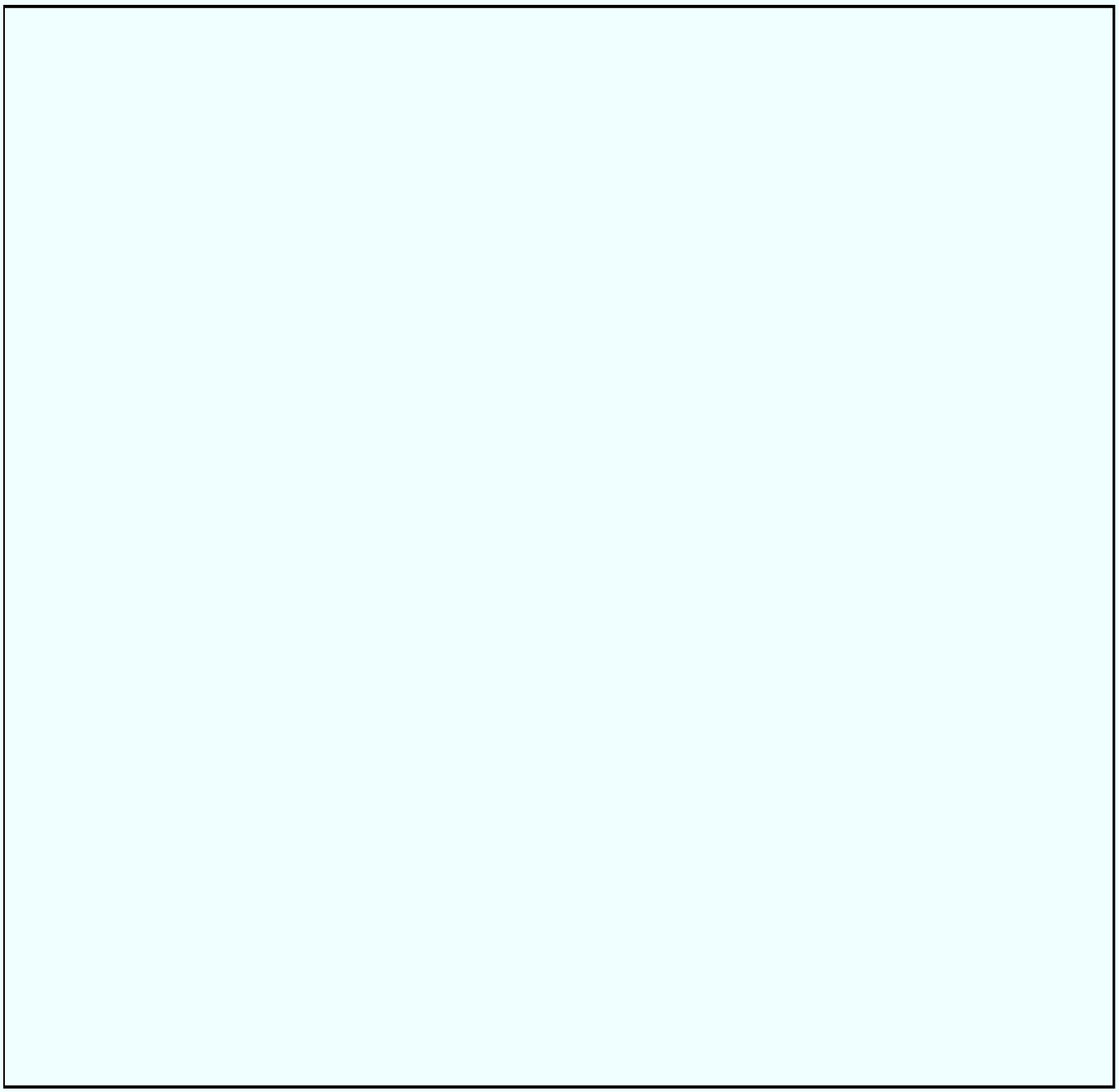


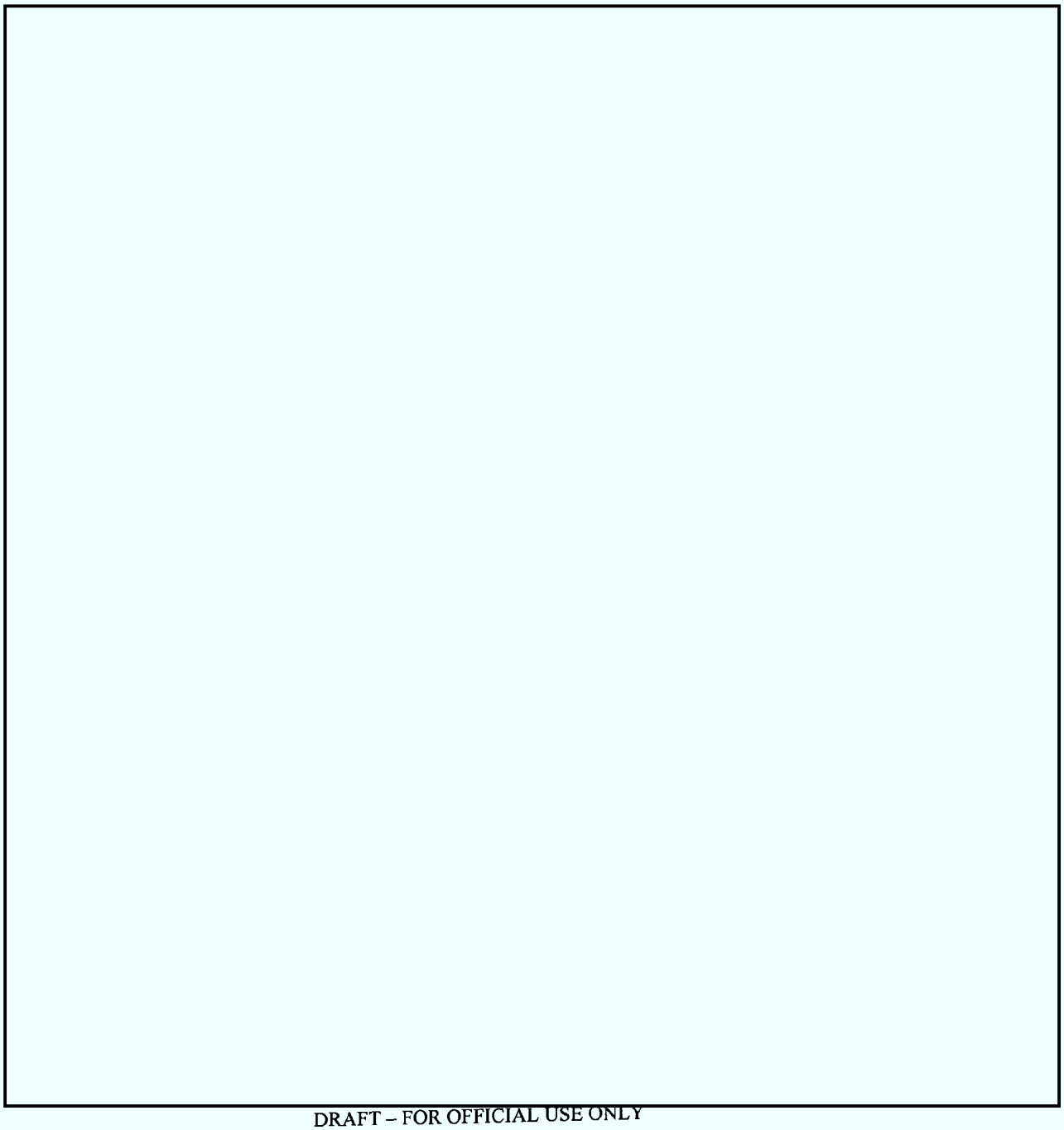


b5

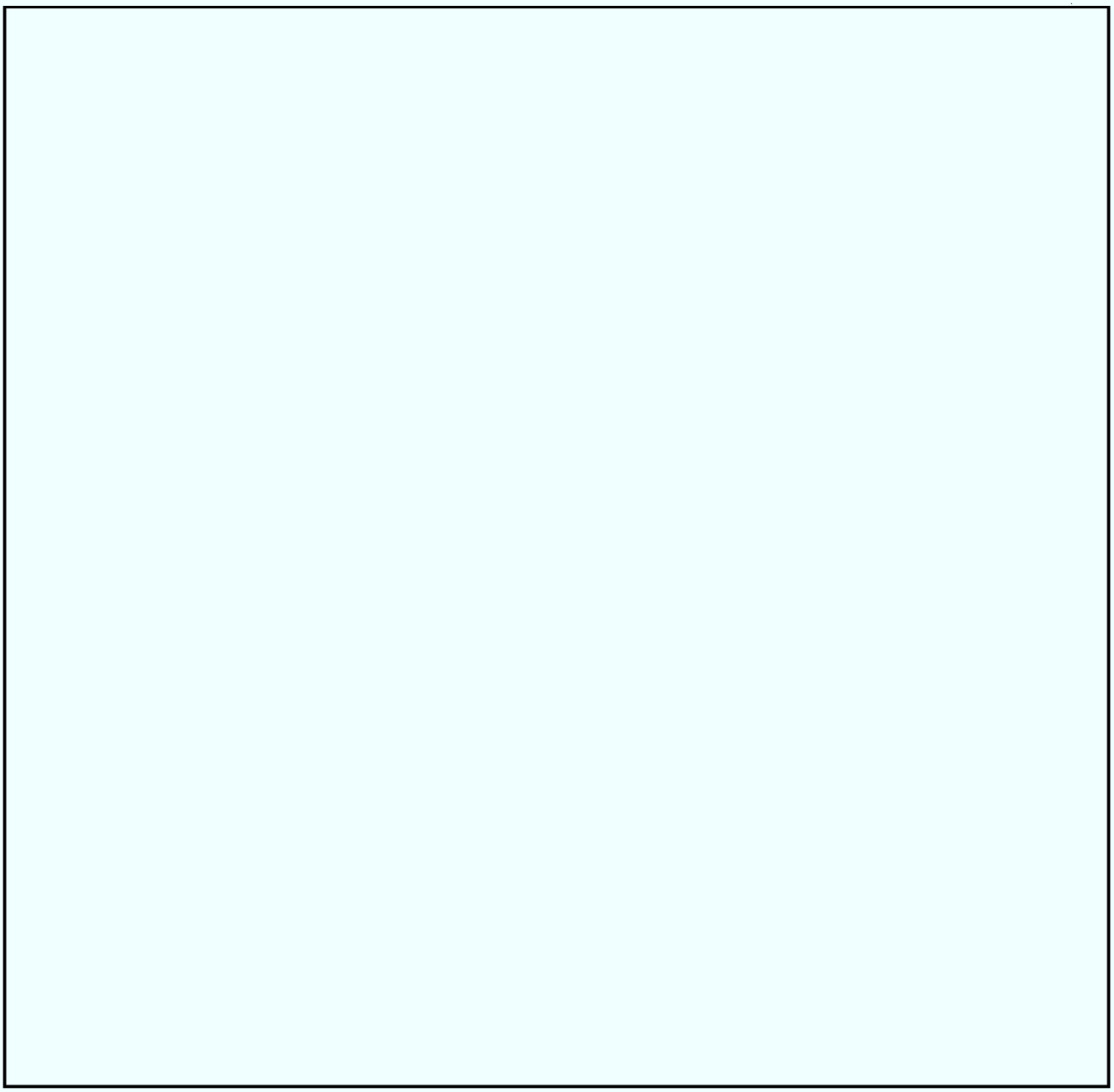


b5

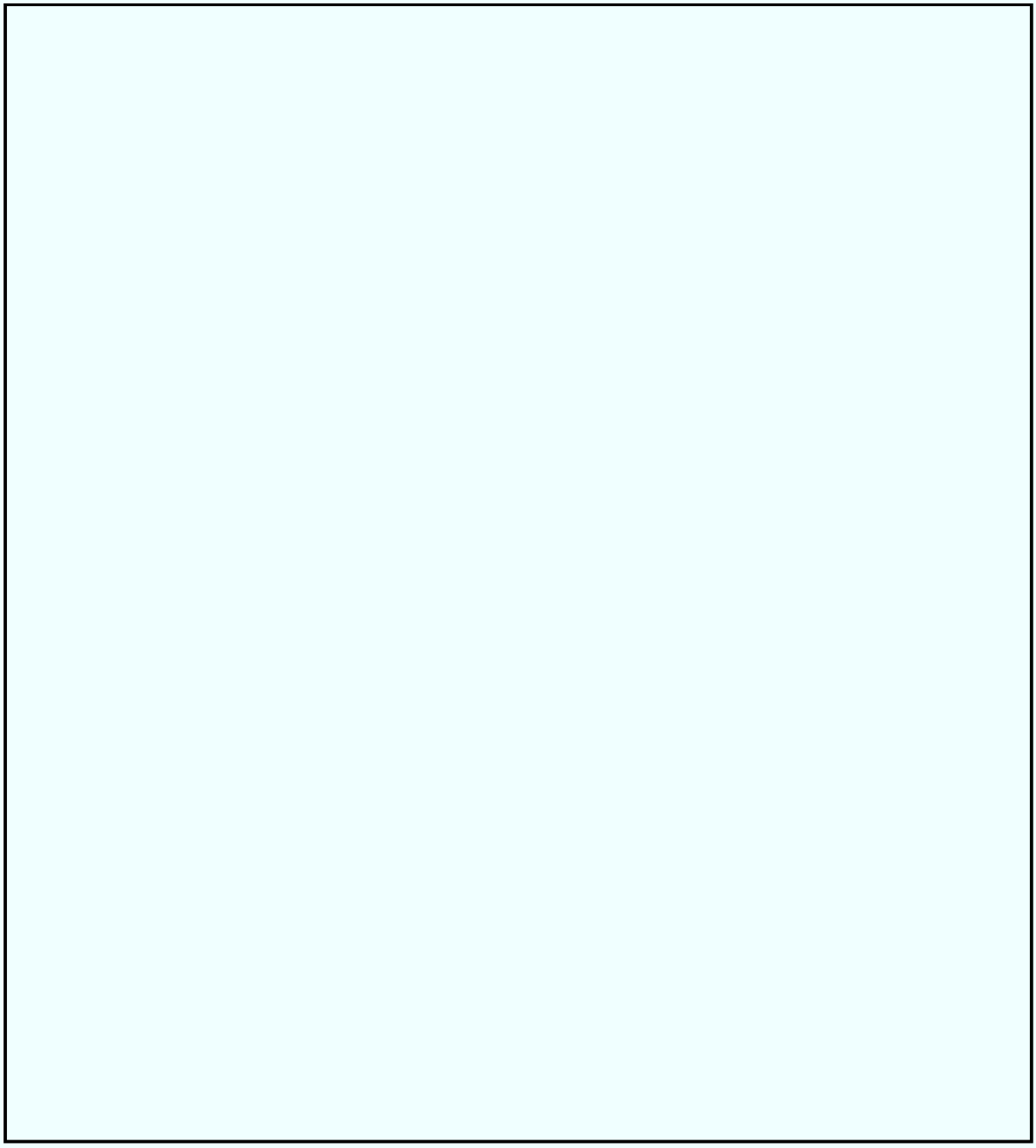




b5

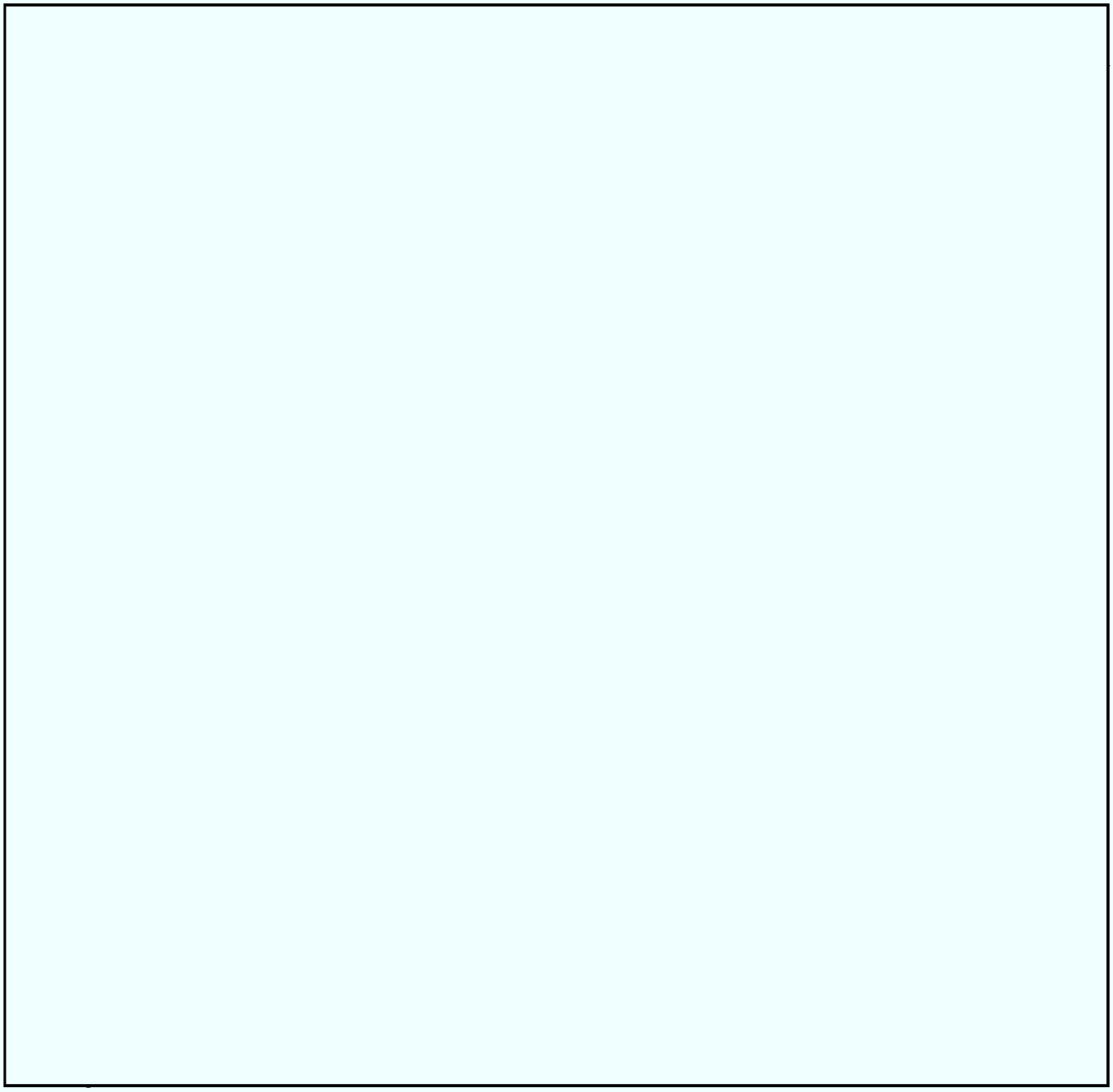


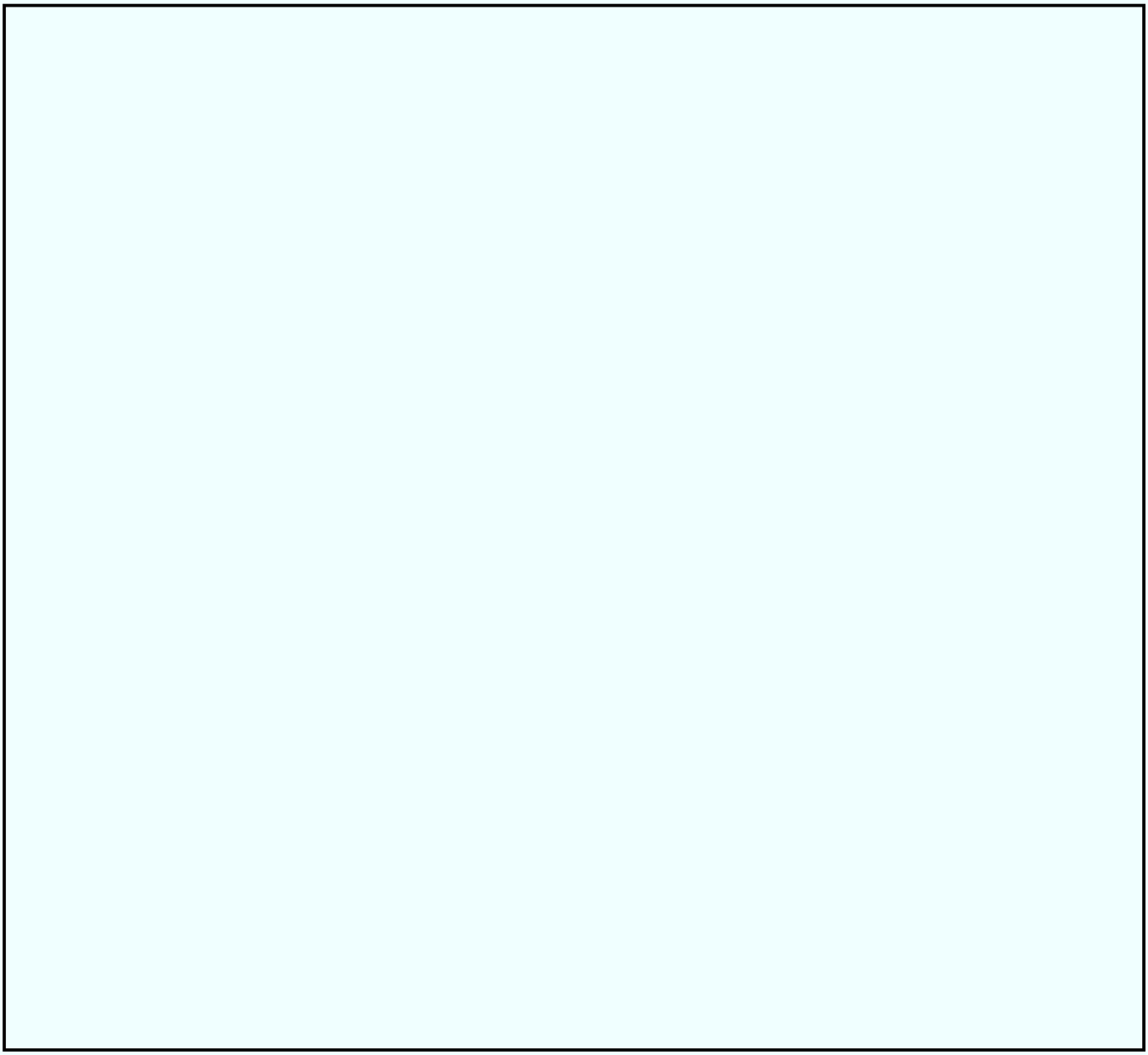
b5



b5

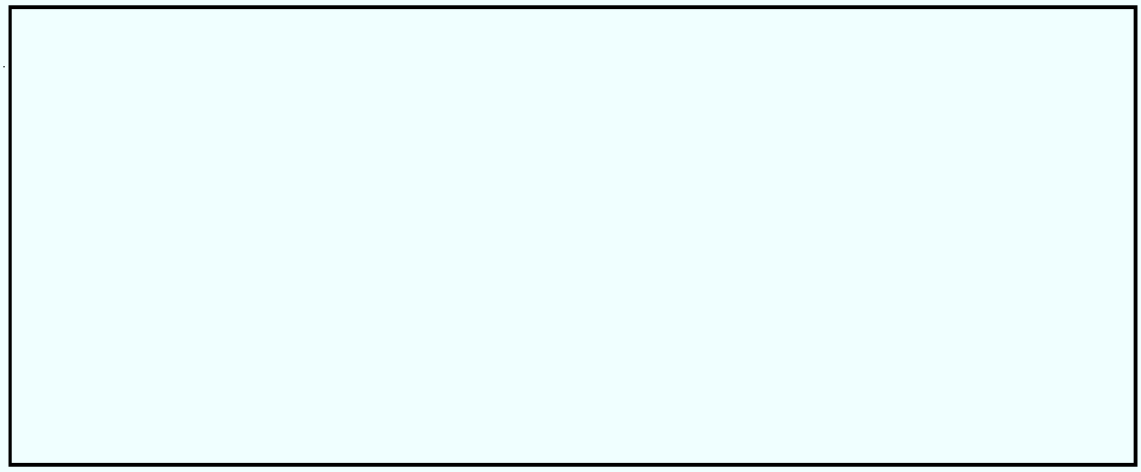
PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT





PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5



b5

b6
b7C

RE Intel Manual.txt

MessageFrom: [redacted] (OGC) (FBI)
Sent: Monday, August 23, 2004 8:44 AM
To: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI)
Cc: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC)(FBI); KELLEY, PATRICK W. (OGC) (FBI)
Subject: RE: Intel Manual

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

b5

[redacted]

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Thursday, August 19, 2004 6:25 PM
To: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI)
Cc: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC)(FBI); KELLEY, PATRICK W. (OGC) (FBI)

b6
b7C

Subject: RE: Intel Manual

b5
b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Thursday, August 19, 2004 5:55 PM
To: [redacted] (OGC) (FBI)
Cc: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC)(FBI); [redacted] (OGC) (FBI); KELLEY, PATRICK W. (OGC) (FBI)
Subject: RE: Intel Manual

b6
b7C

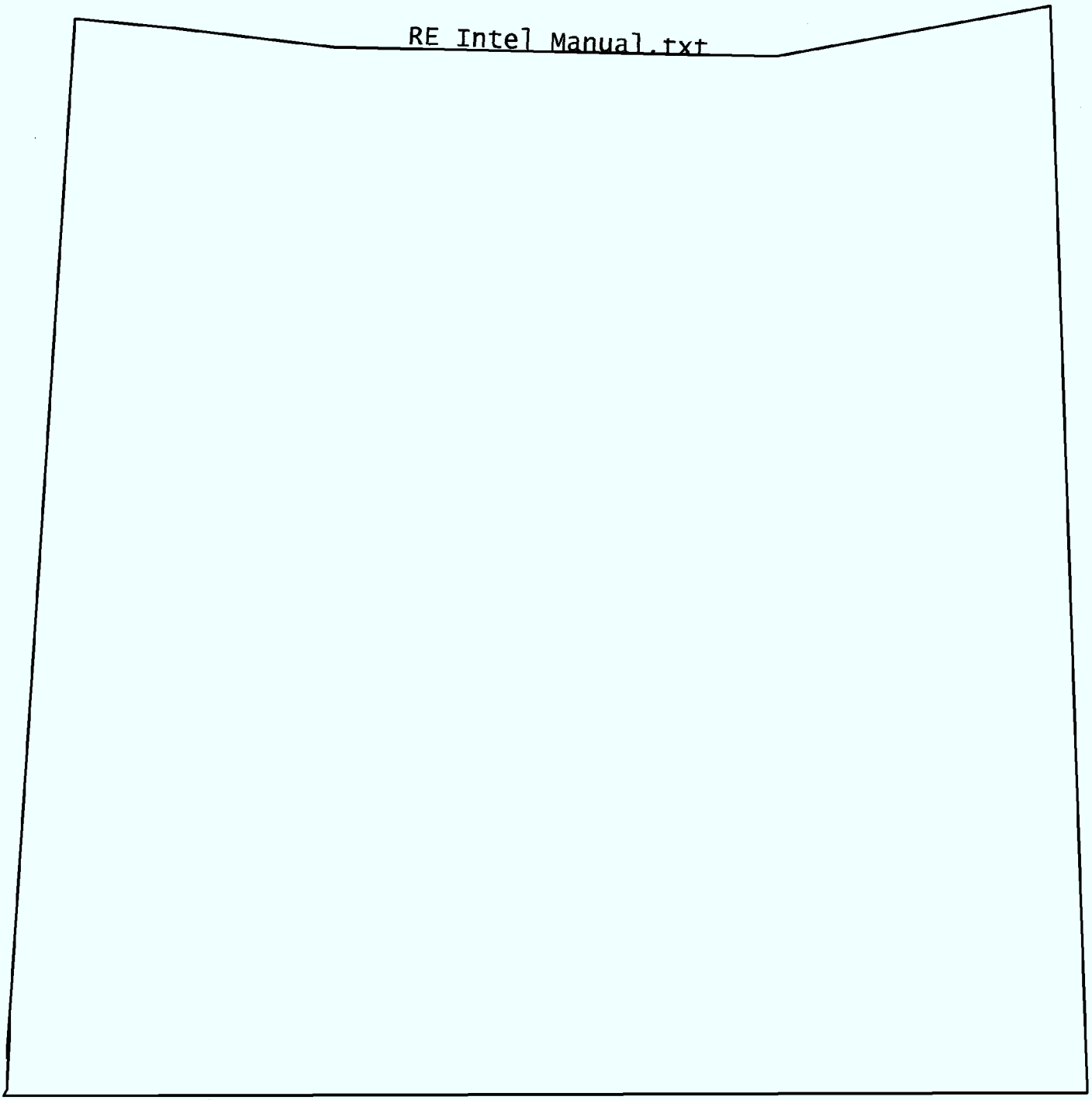
b5
b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]

b5
b6
b7C

RE Intel Manual.txt



-----Original Message-----
From: (OGC) (FBI)
Sent: Monday, August 16, 2004 5:55 PM
To: (OGC) (FBI)

b6
b7C

b6
b7C

RE Intel Manual.txt

Cc: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC)(FBI); [redacted] (OGC) (FBI); KELLEY, PATRICK W. (OGC) (FBI)

Subject: Intel Manual

b5
b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]

[redacted]

Office of the General Counsel [redacted]

b6
b7C
b2

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

b6
b7C

b5

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 10-06-2005 BY 65179 DMH/JHF 05-CV-0845

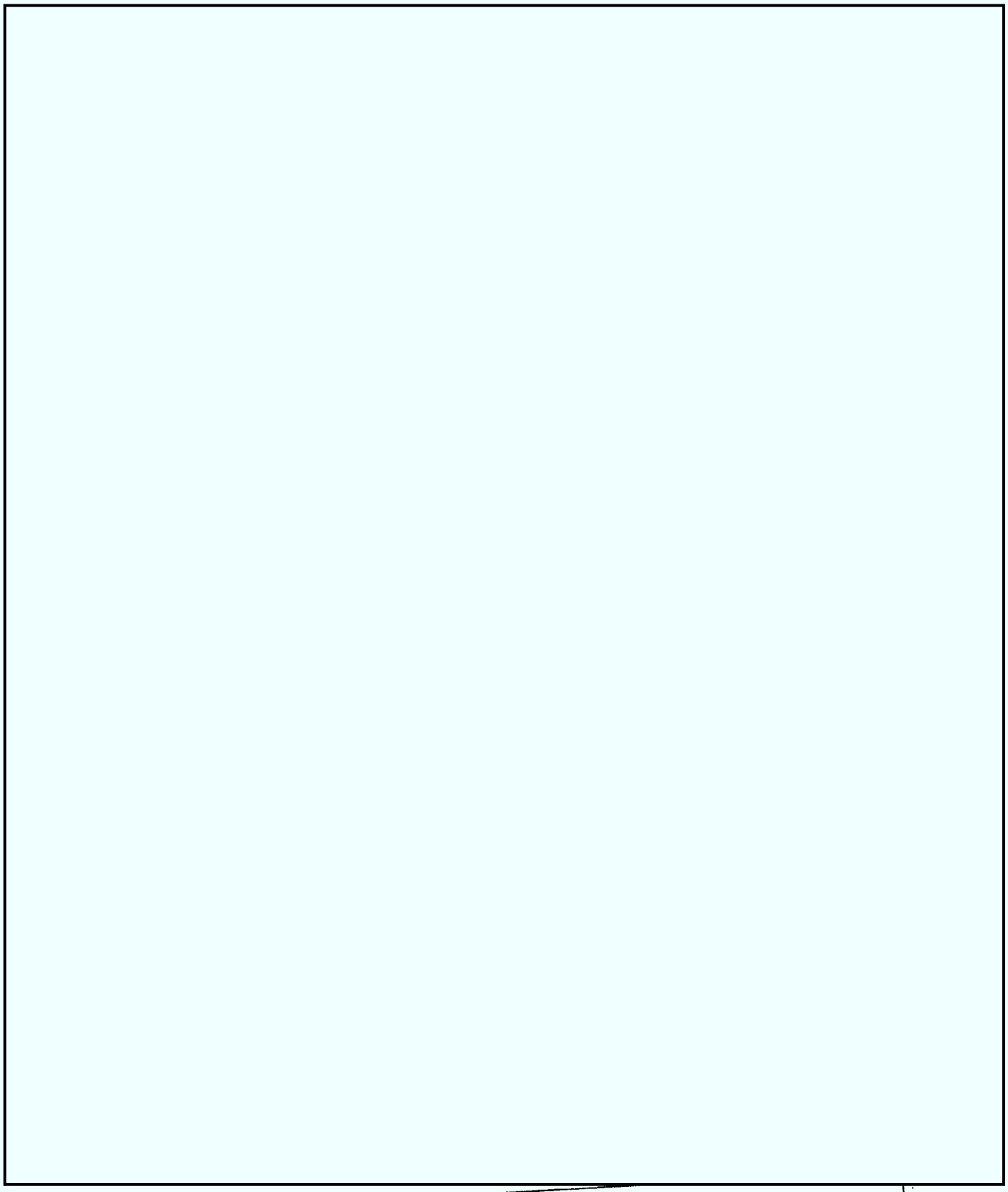
Comments from [redacted] 19 August, 5:55 pm

[redacted]

Comments from [redacted] 11 August, 7:40 pm b6 b5
b7C

[redacted]

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT



b5

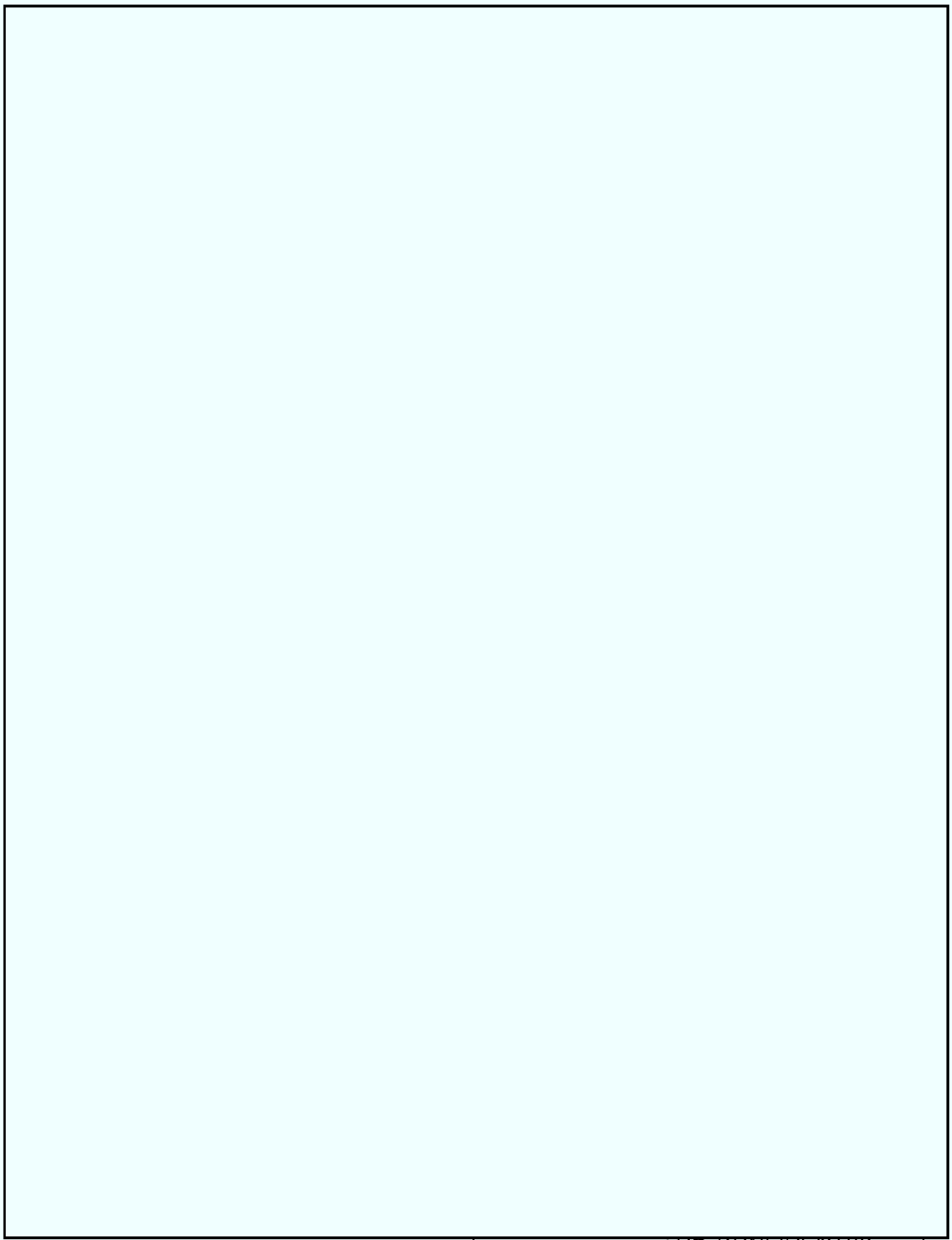
COMMENTS FROM [redacted] NSLB/Policy & Training Unit:

b6
b7C

b5

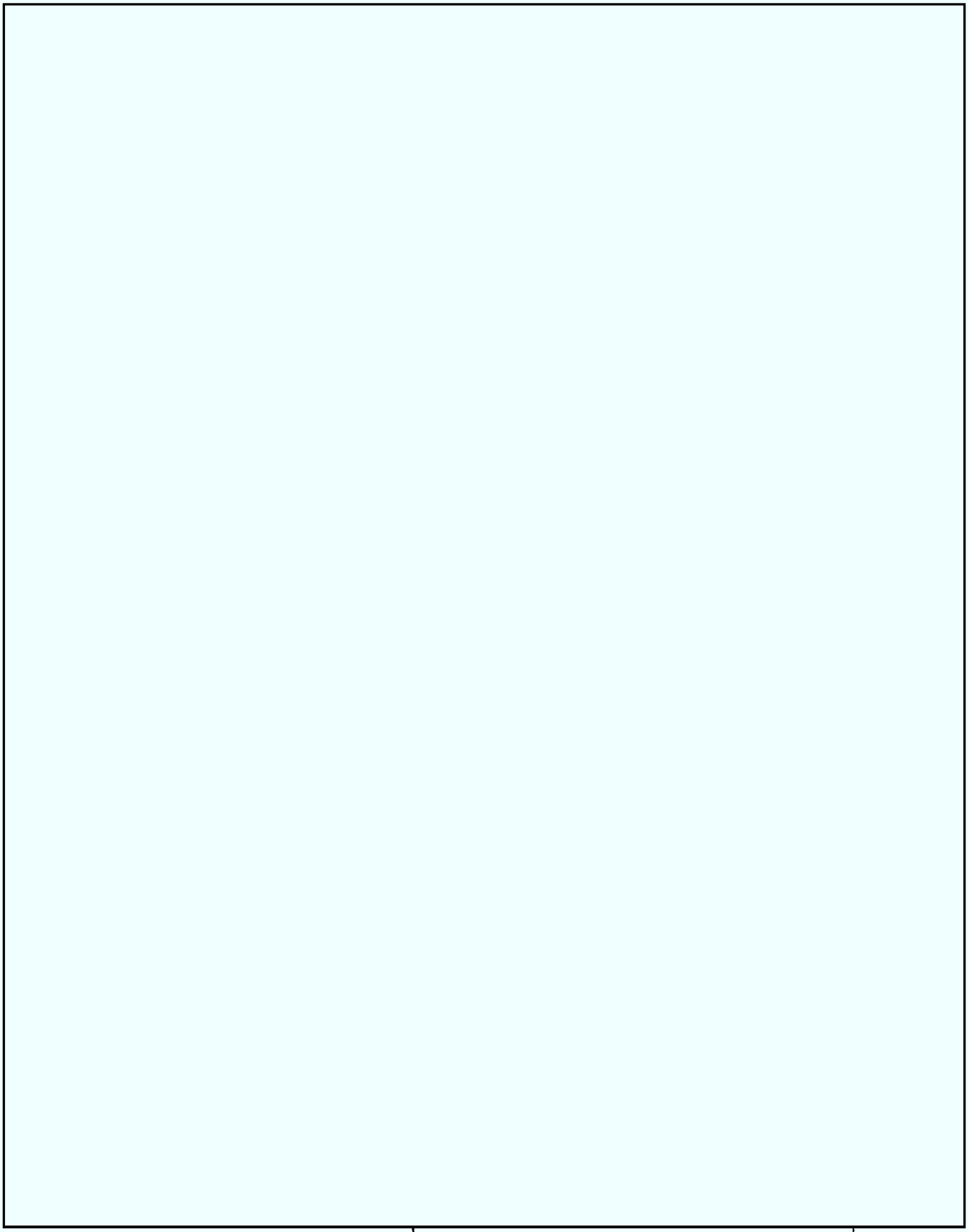
PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5



PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5



PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

DRAFT: 9/23/04 Deleted: 7/29/04

[redacted] b5

[redacted]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 10-06-2005 BY 65179 DMH/JHF 05-CV-0845

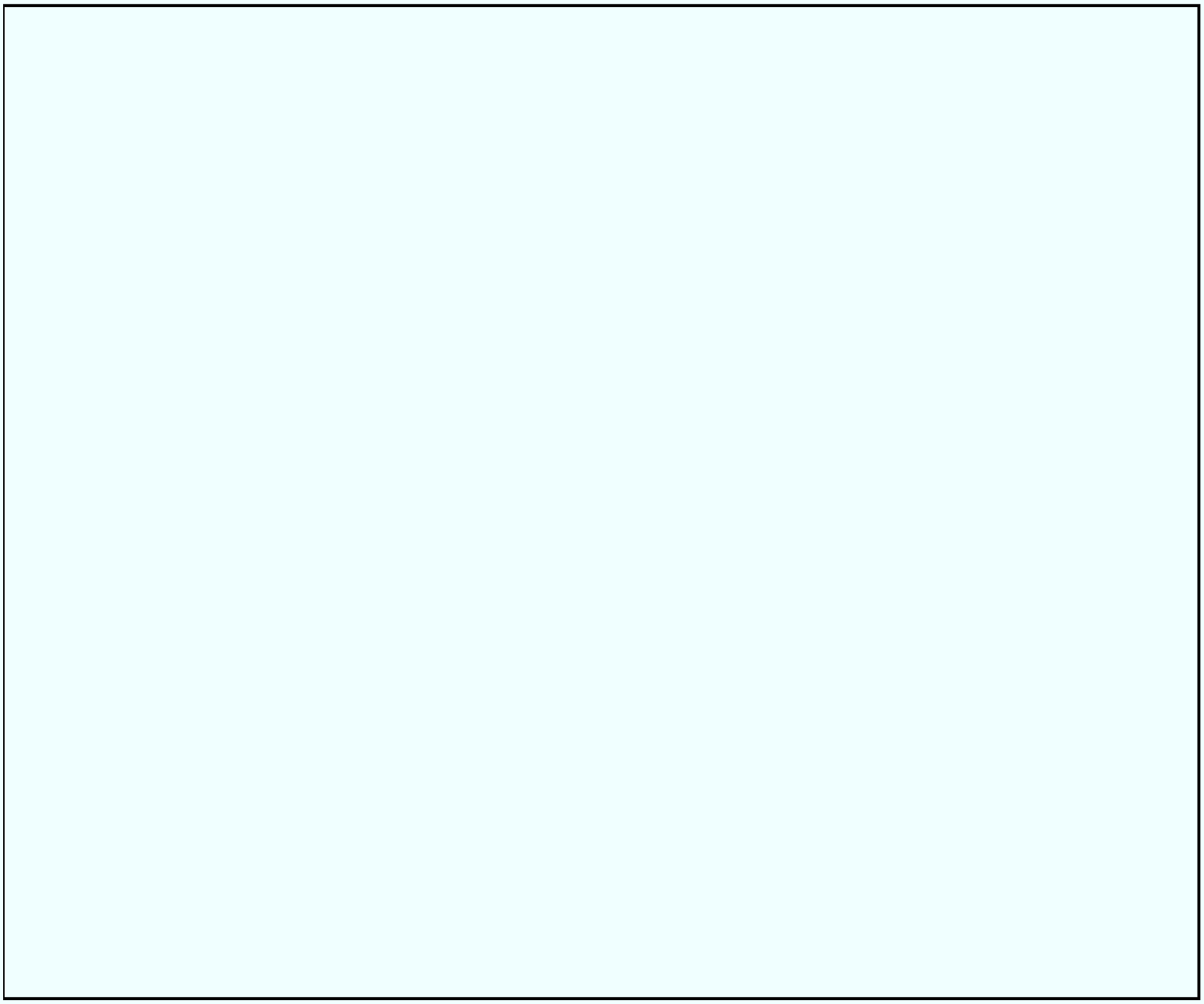
[redacted] b5

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

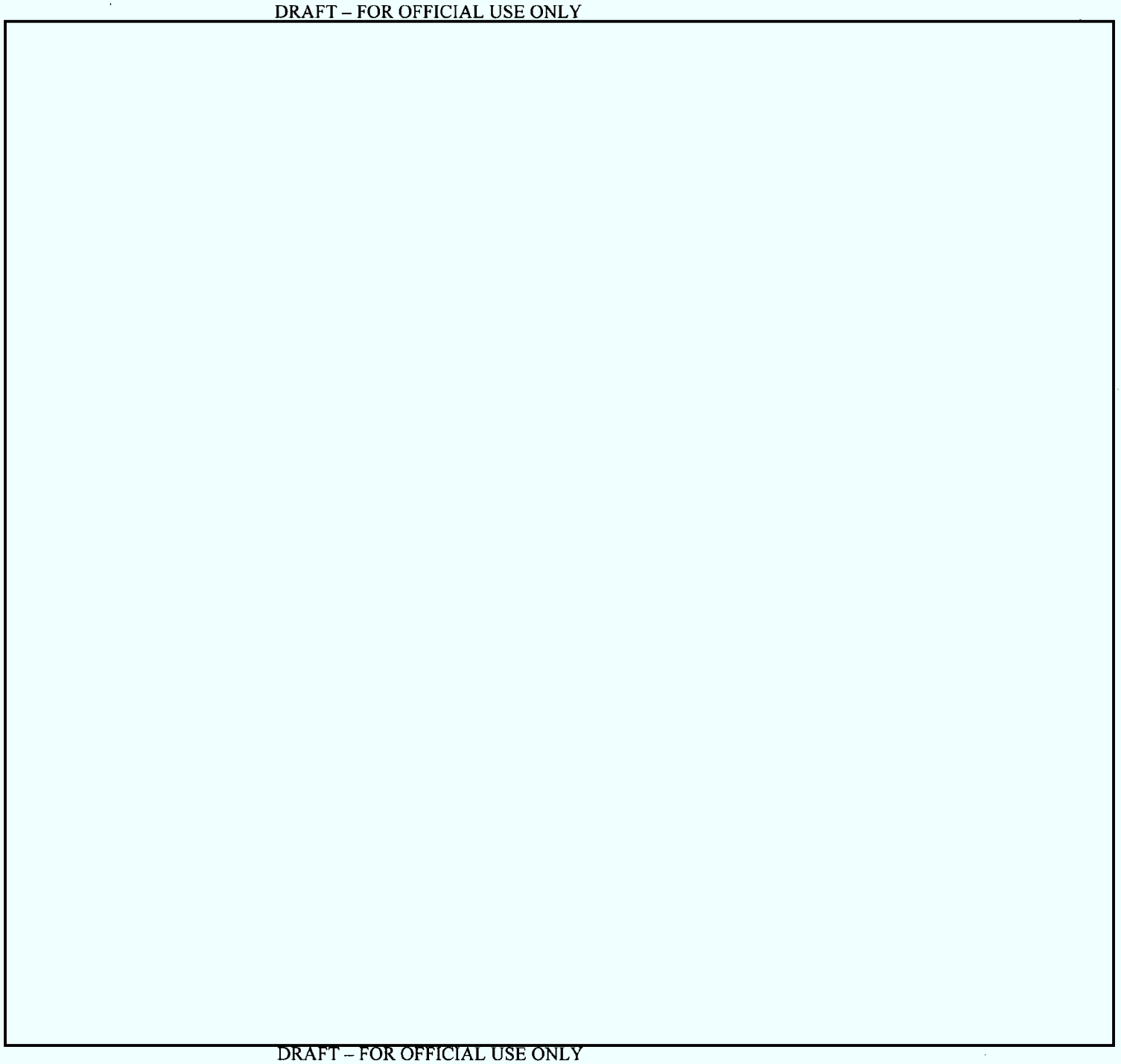
Introduction:

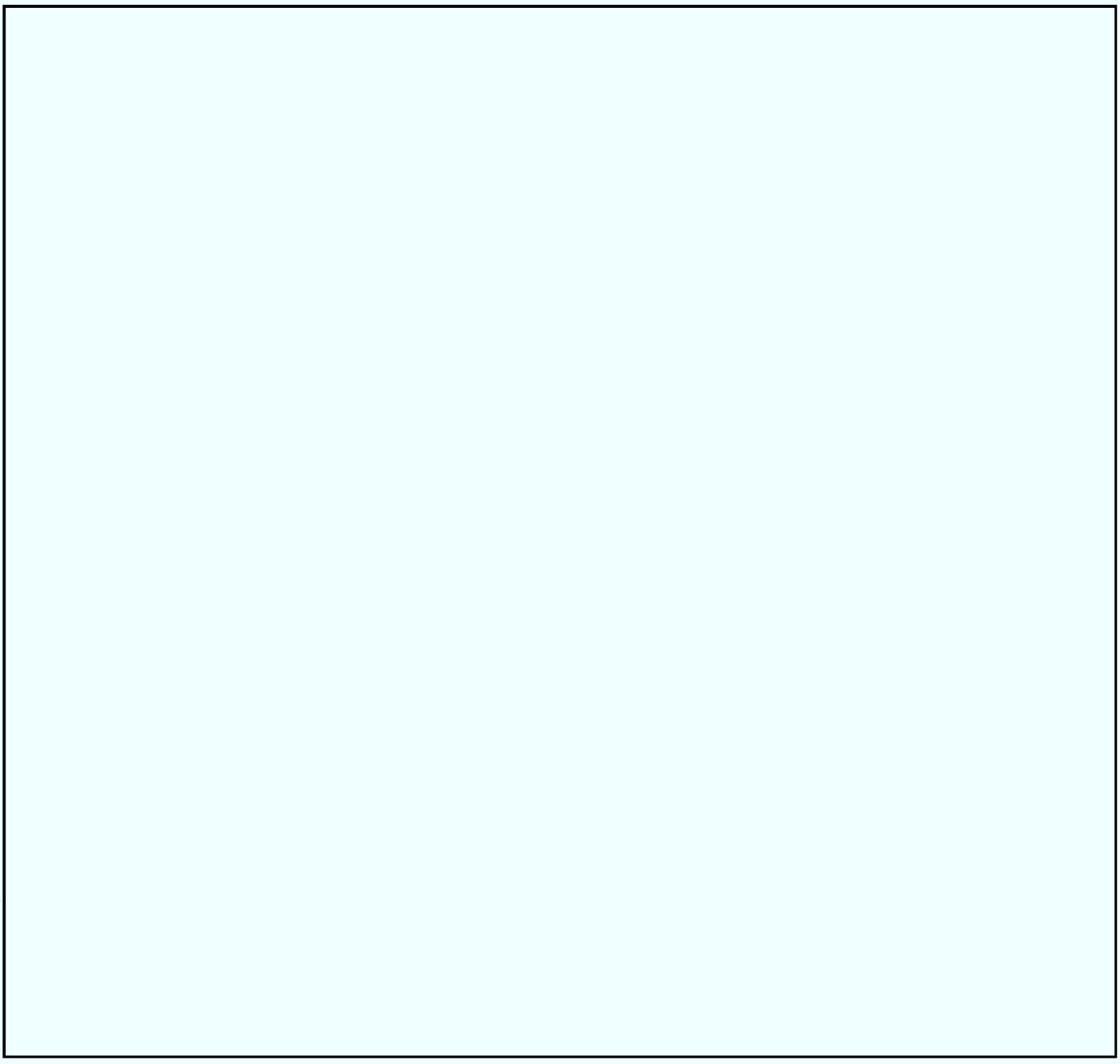
b5

b5

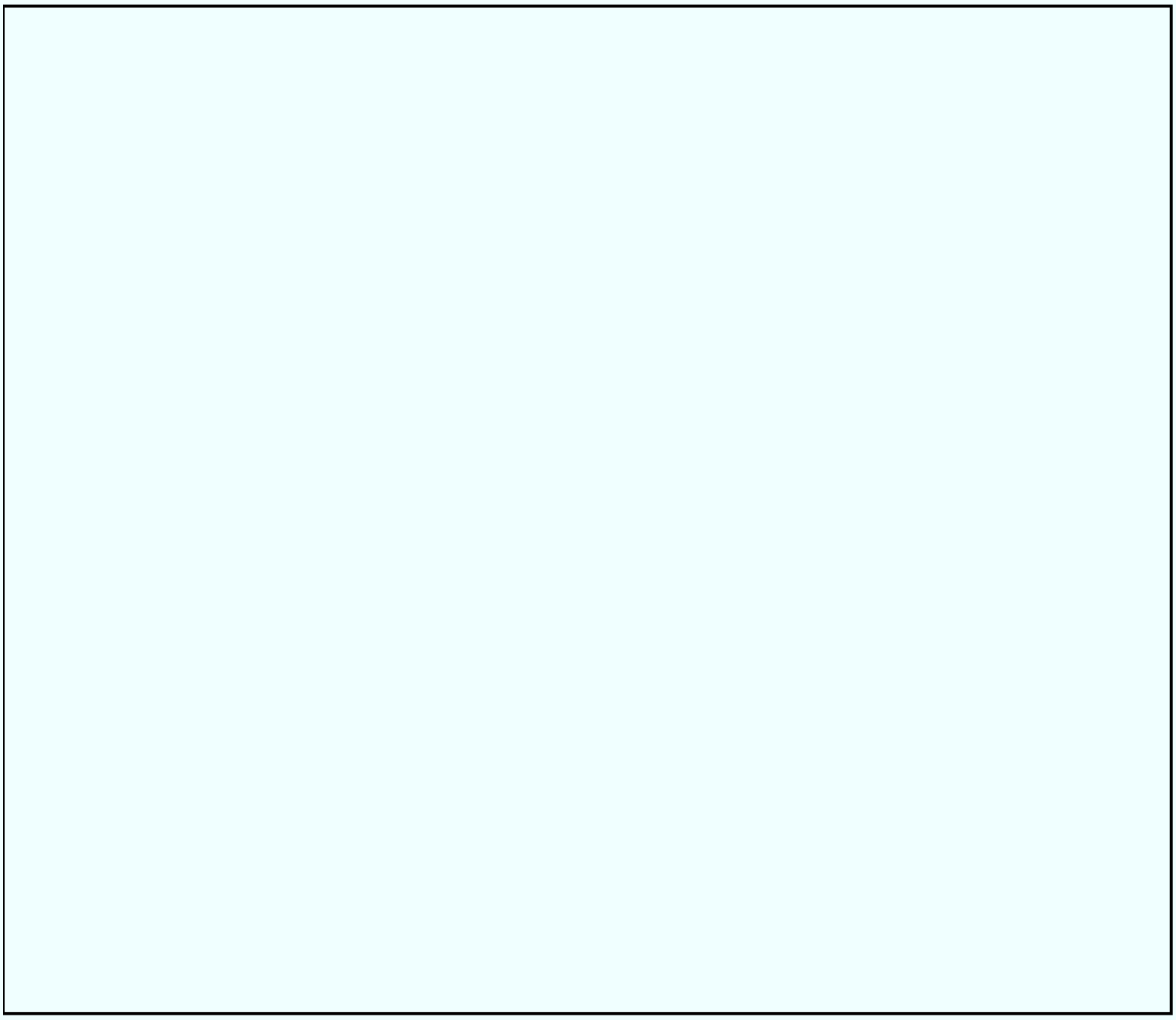


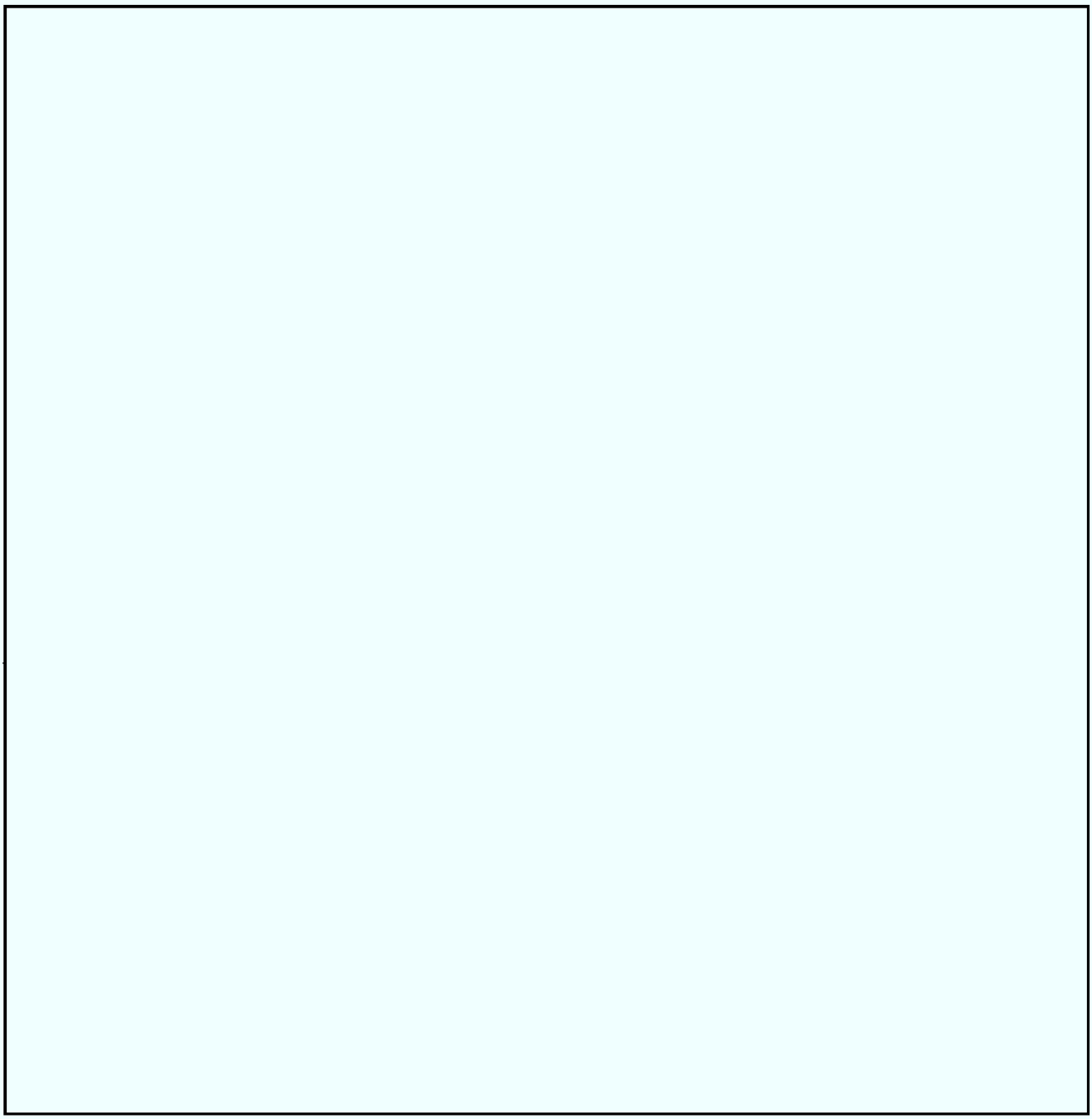
b5



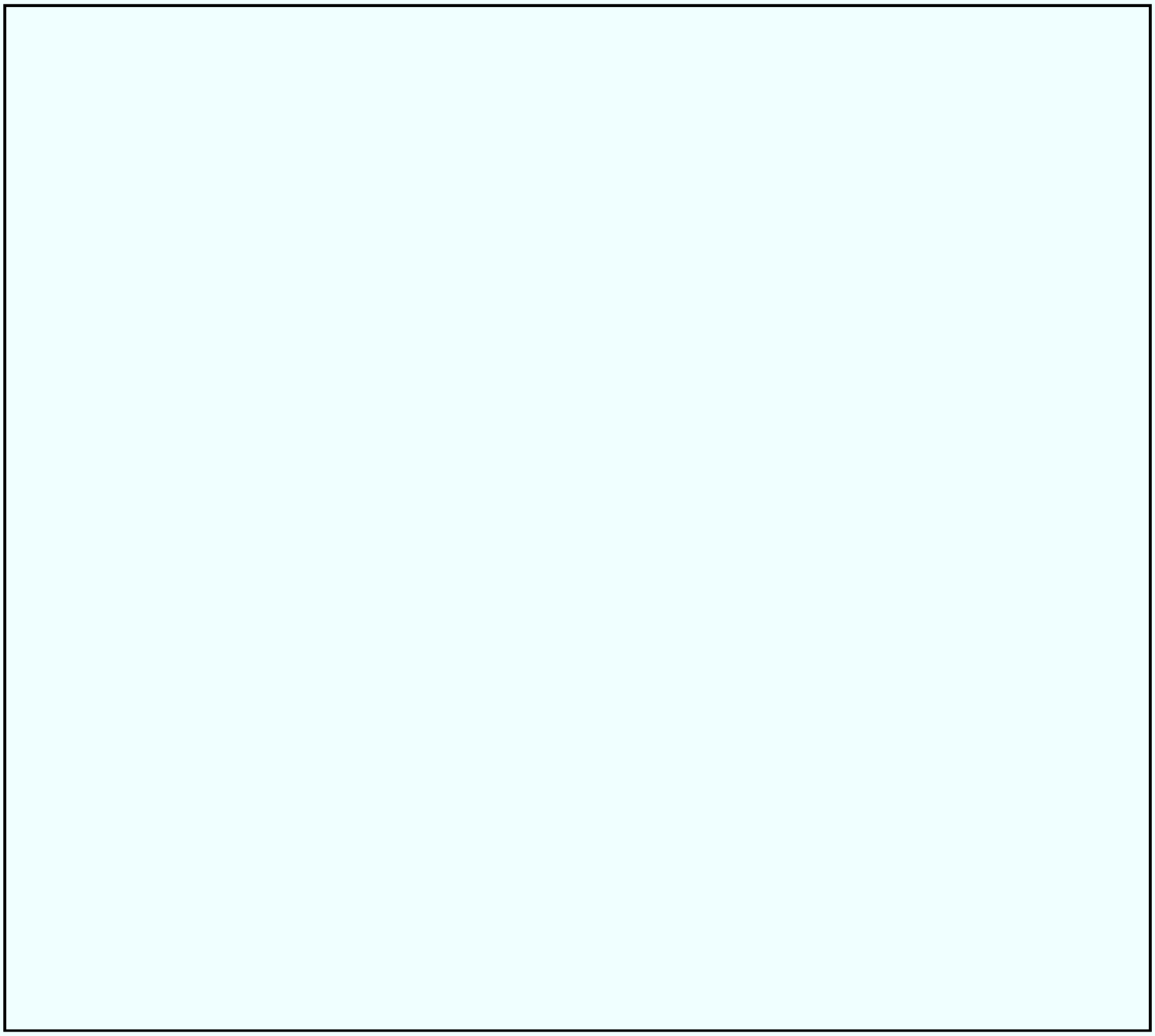


b5

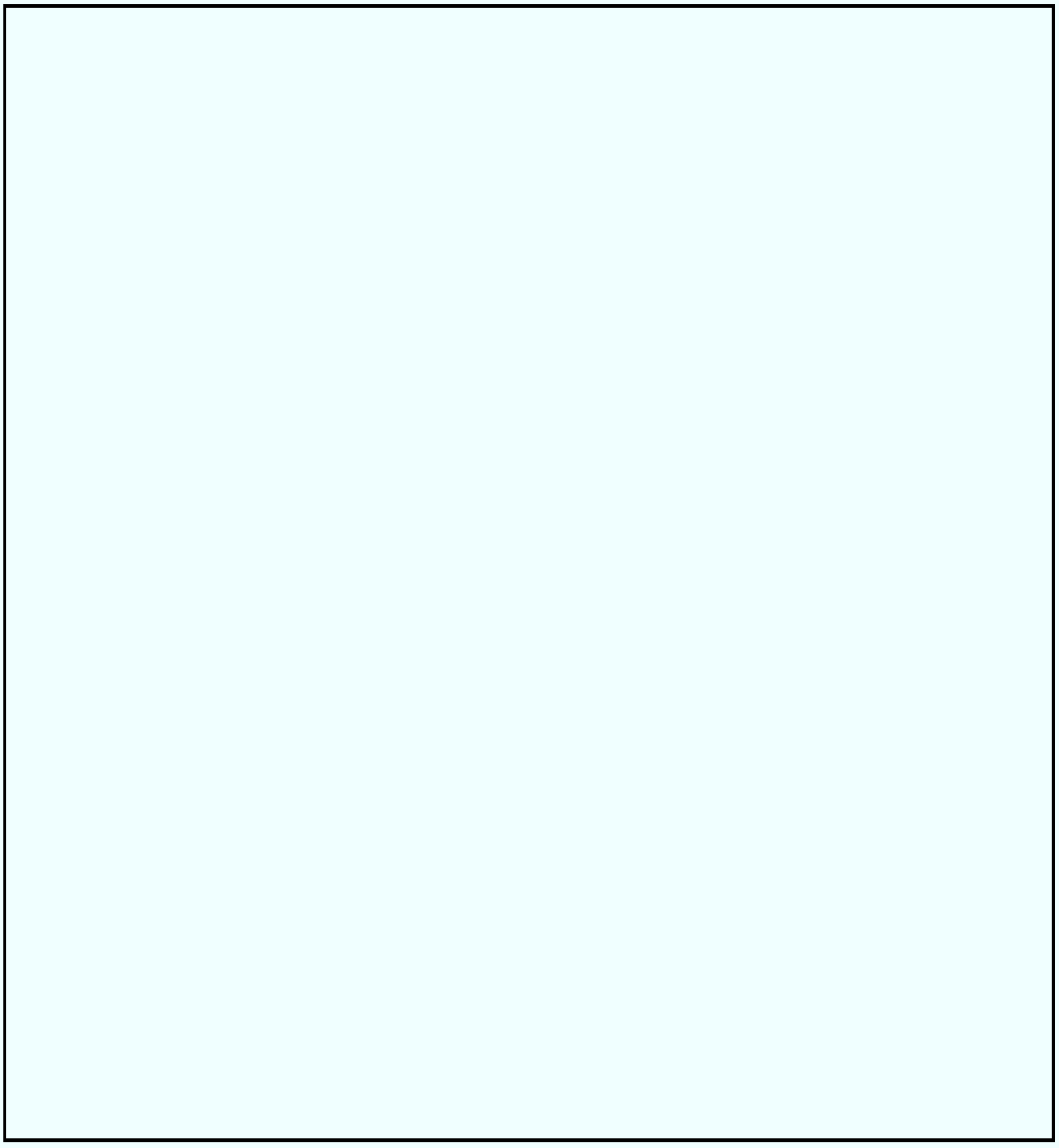




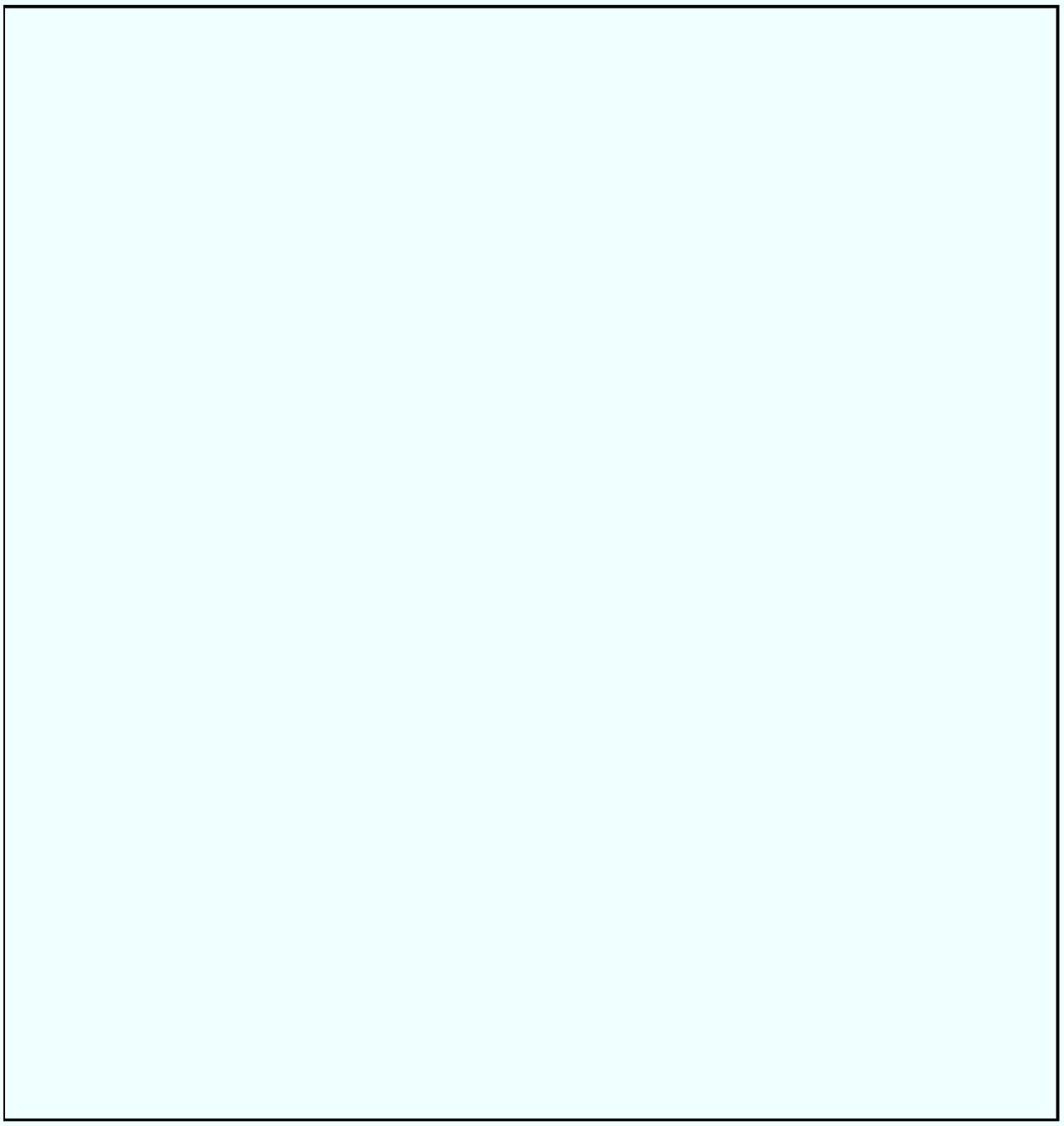
b5



b5



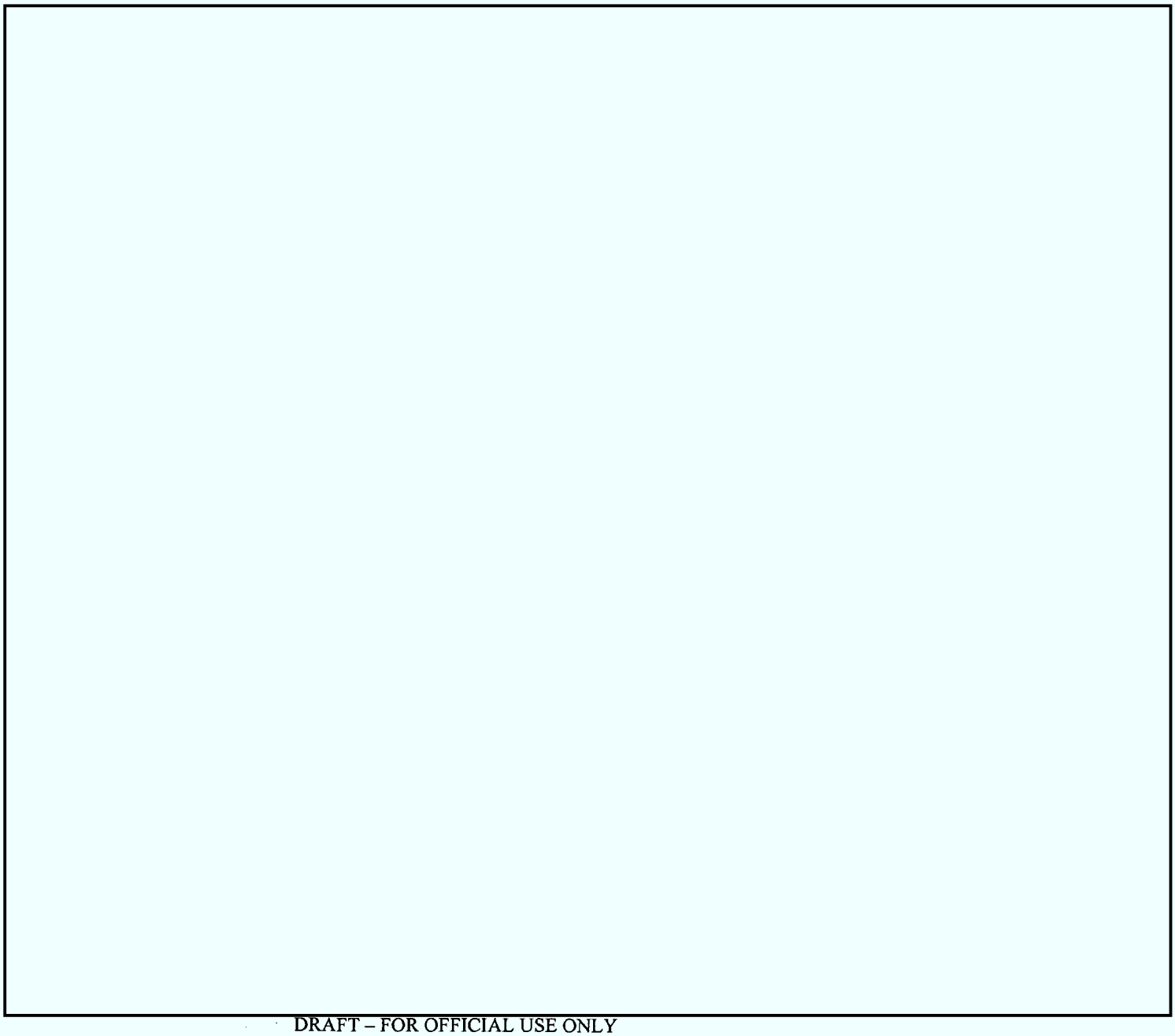
b5

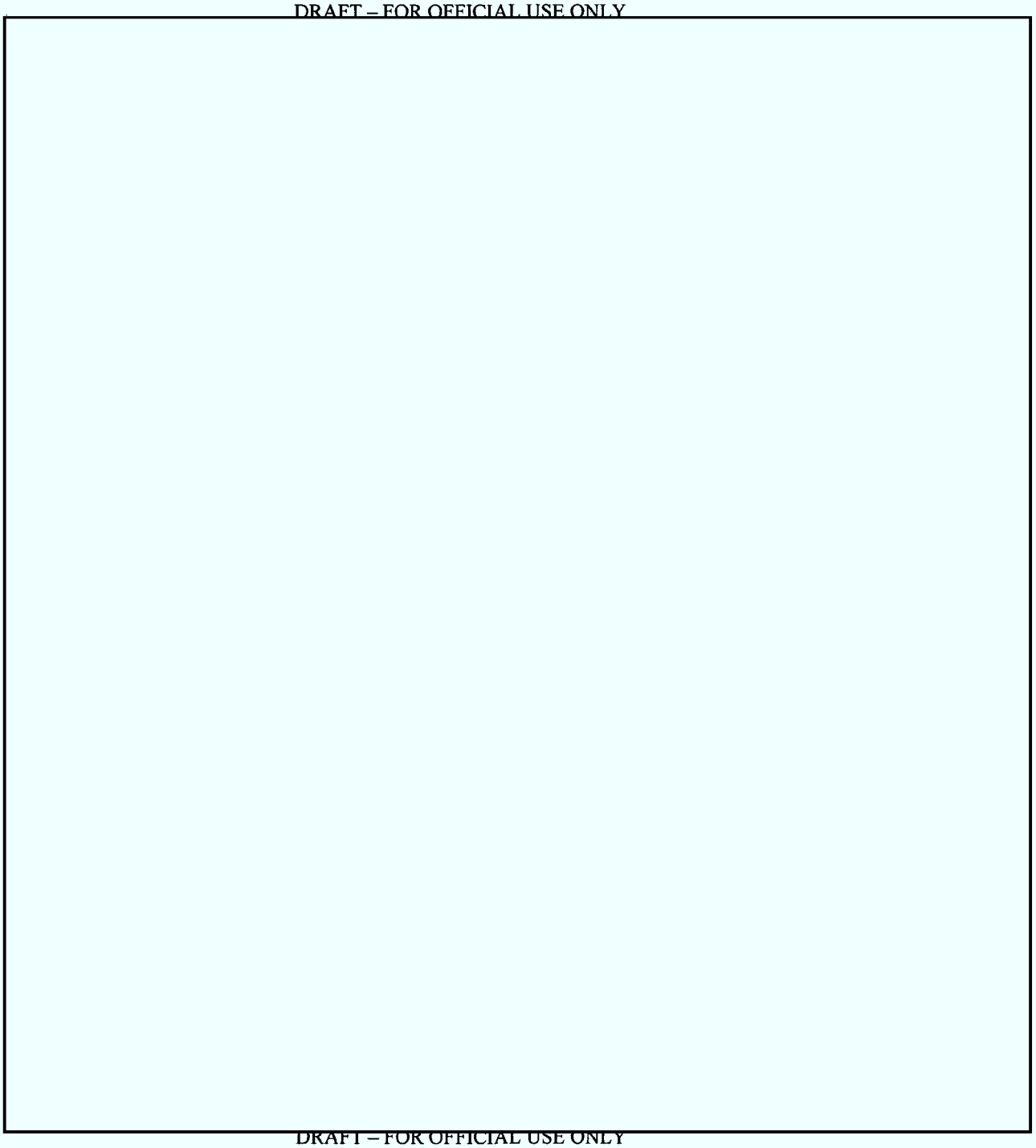


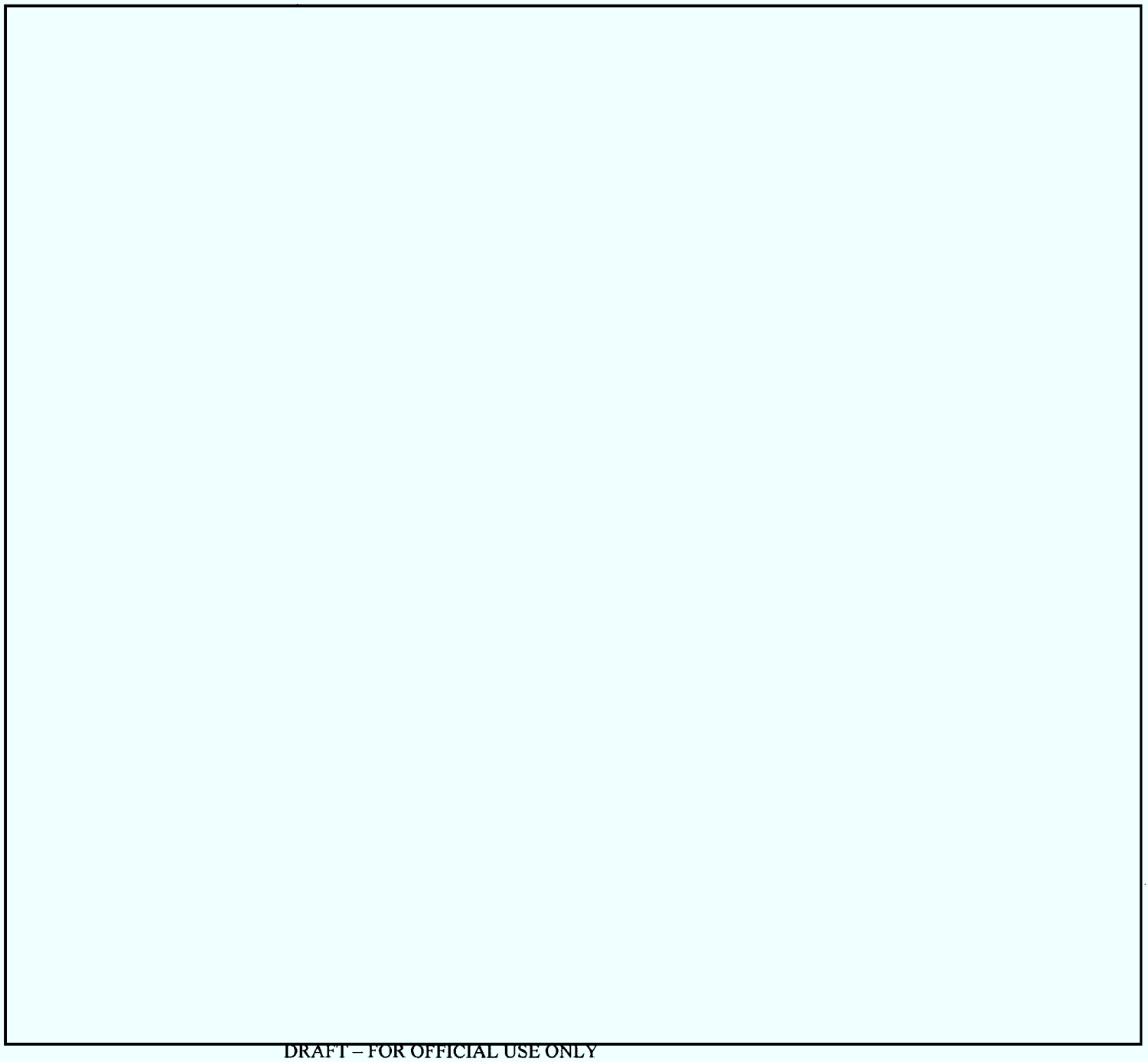
b5

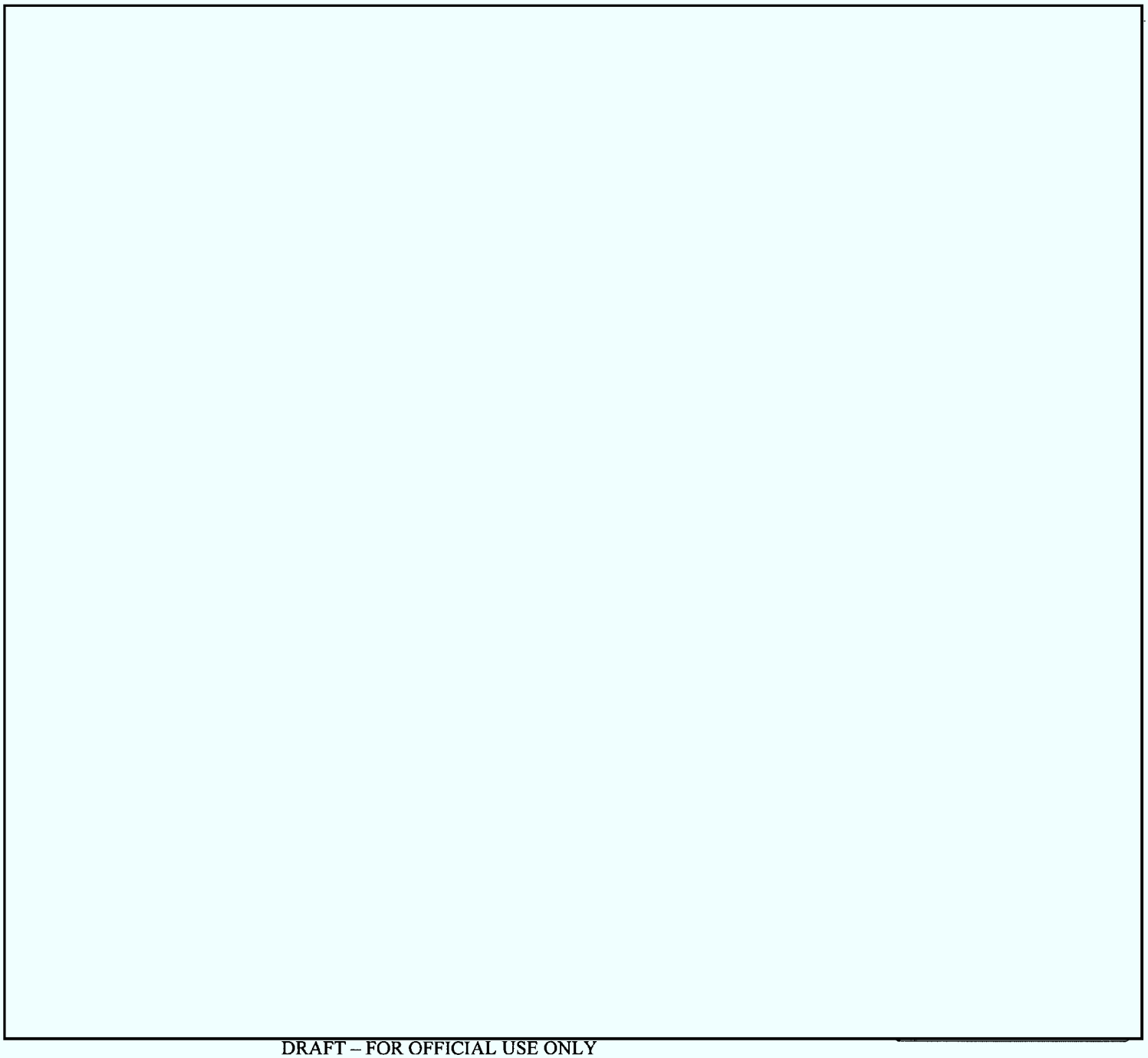
PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5

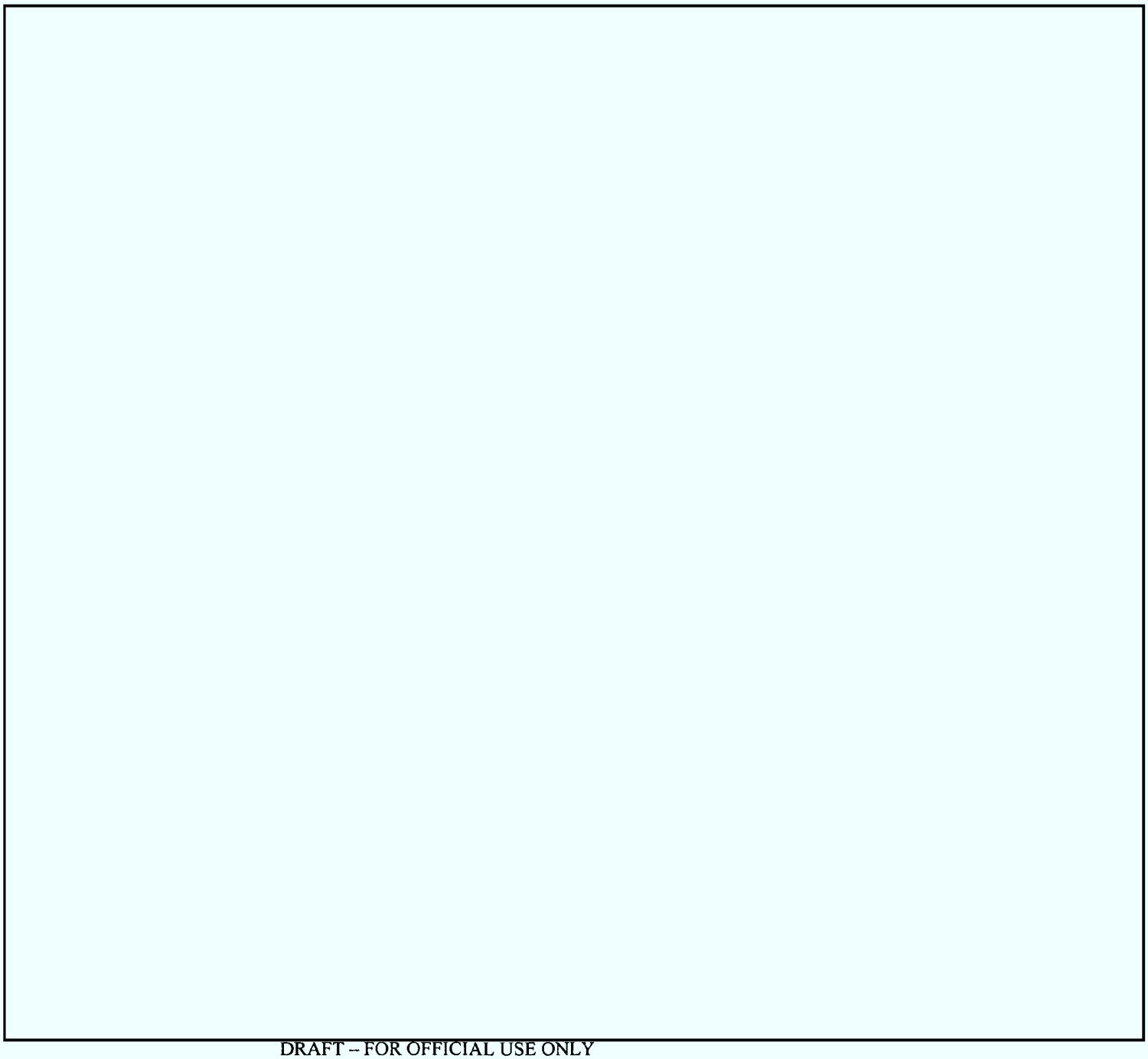






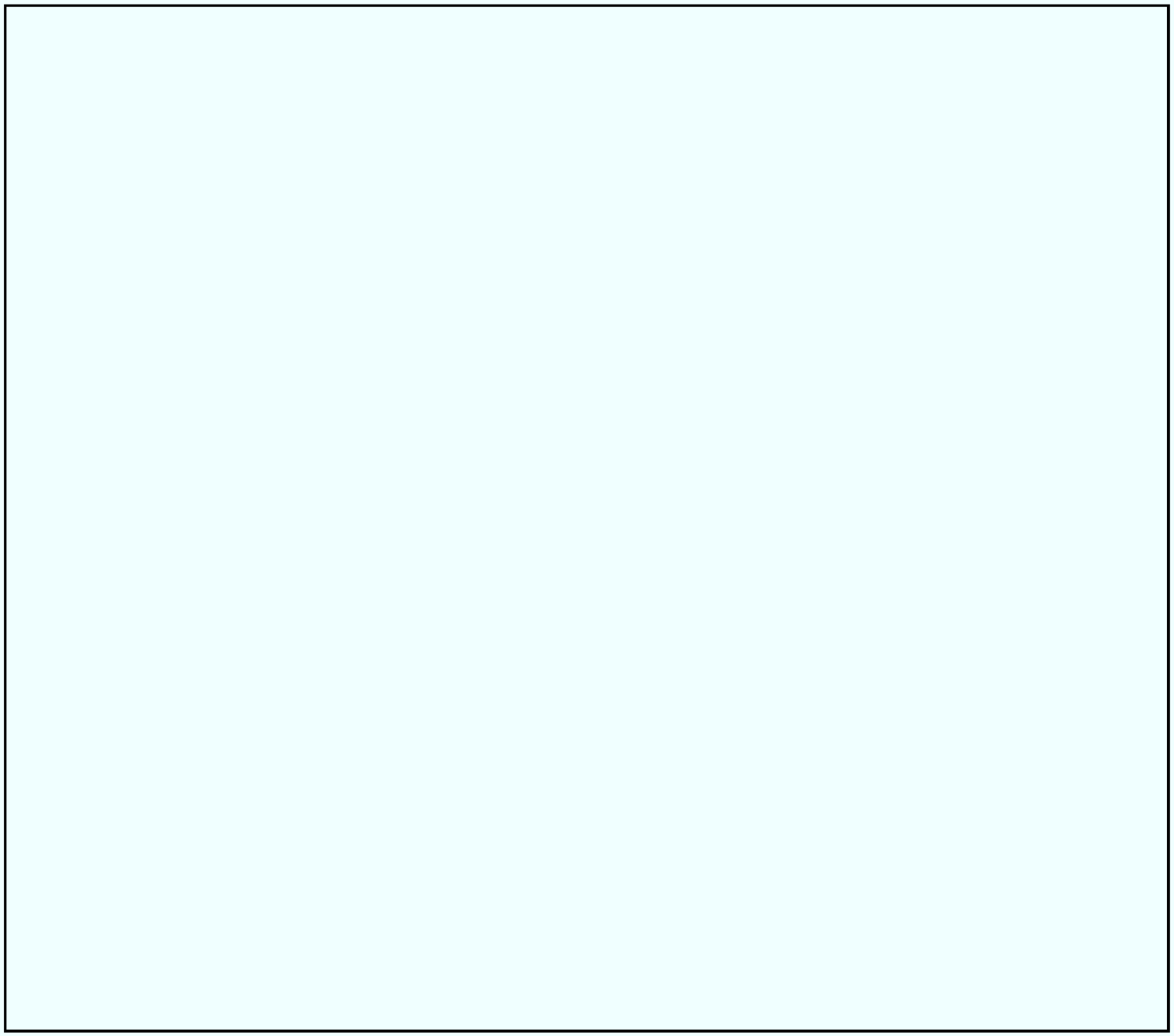


b5

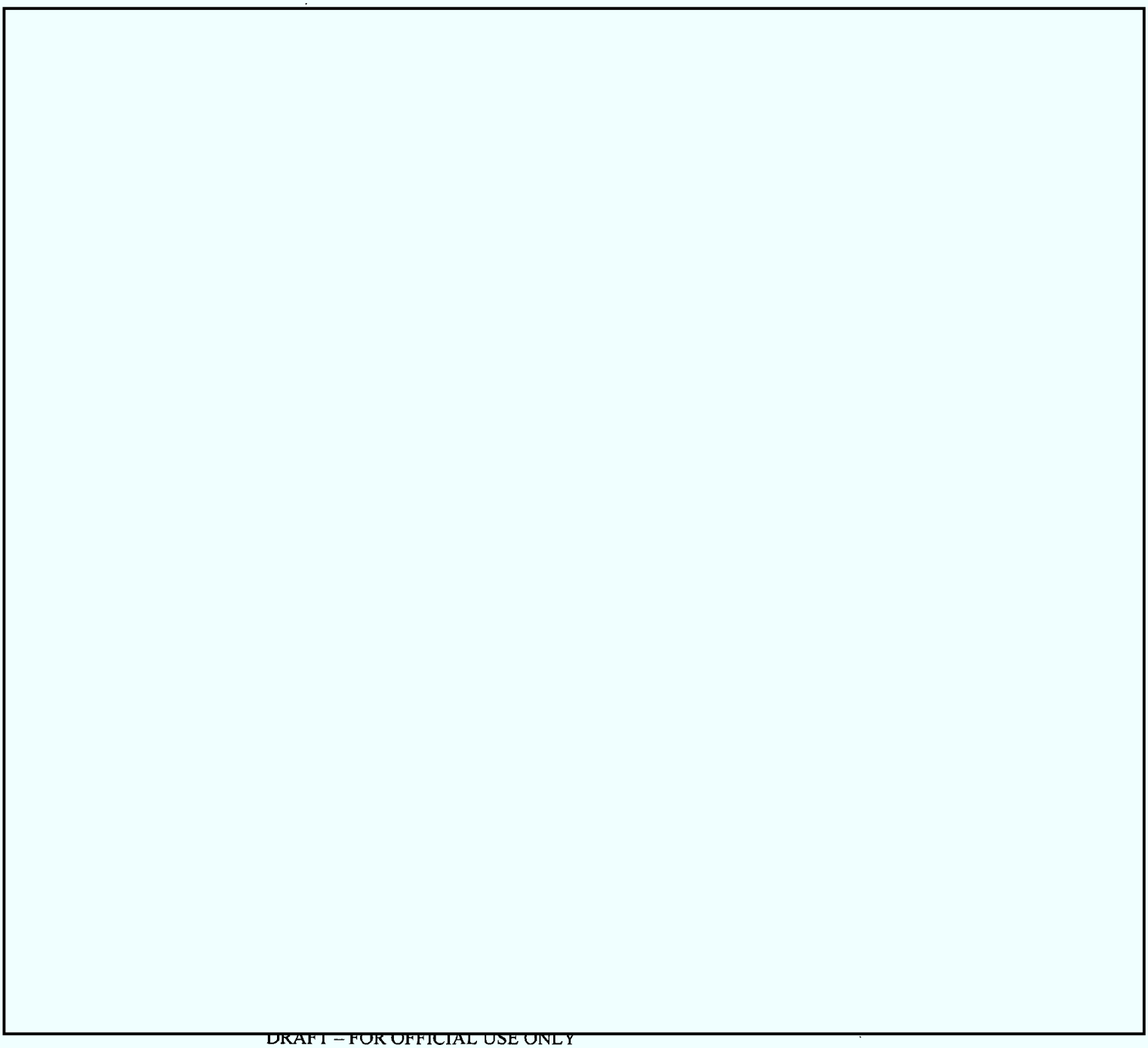


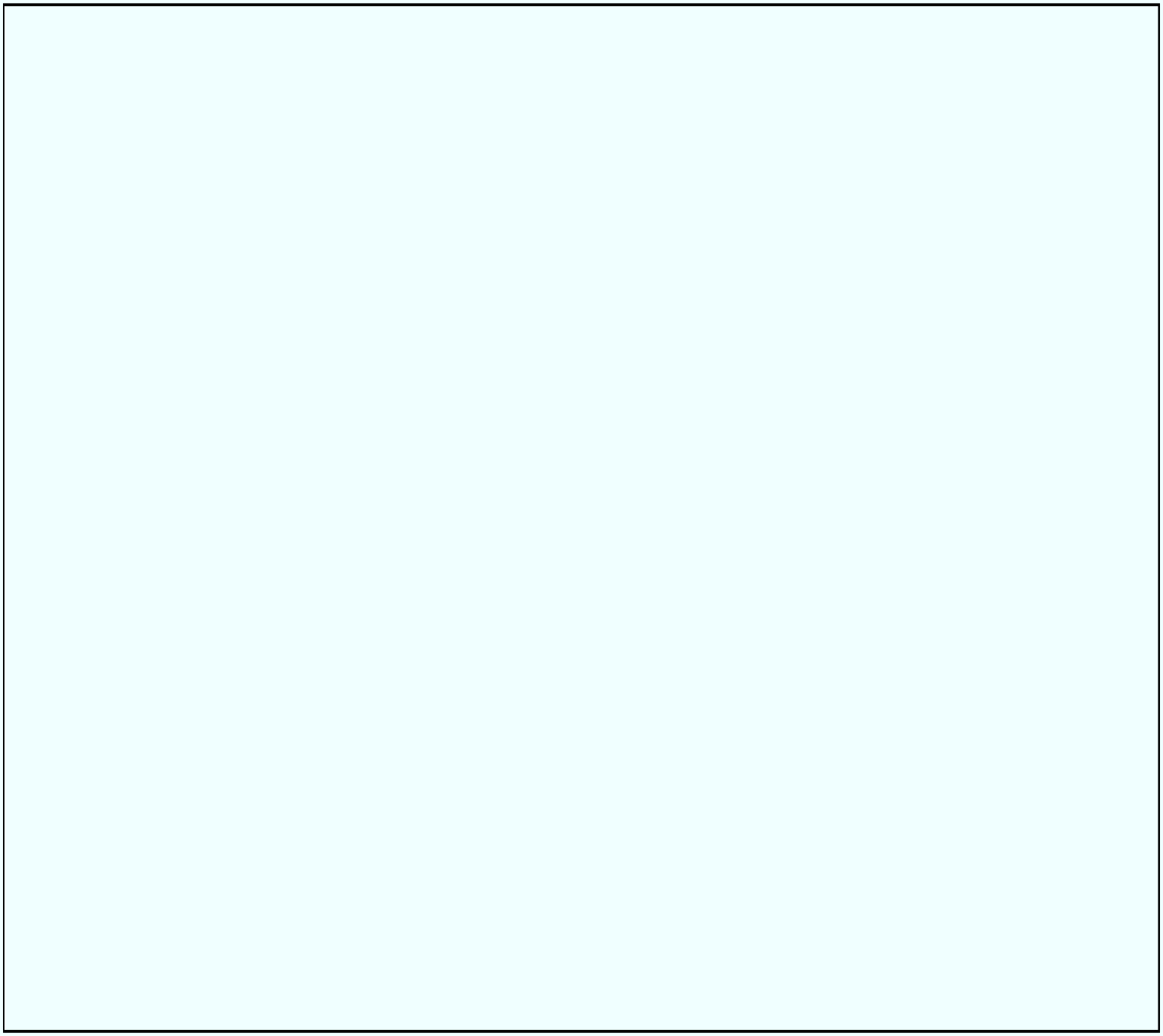
b5

b5

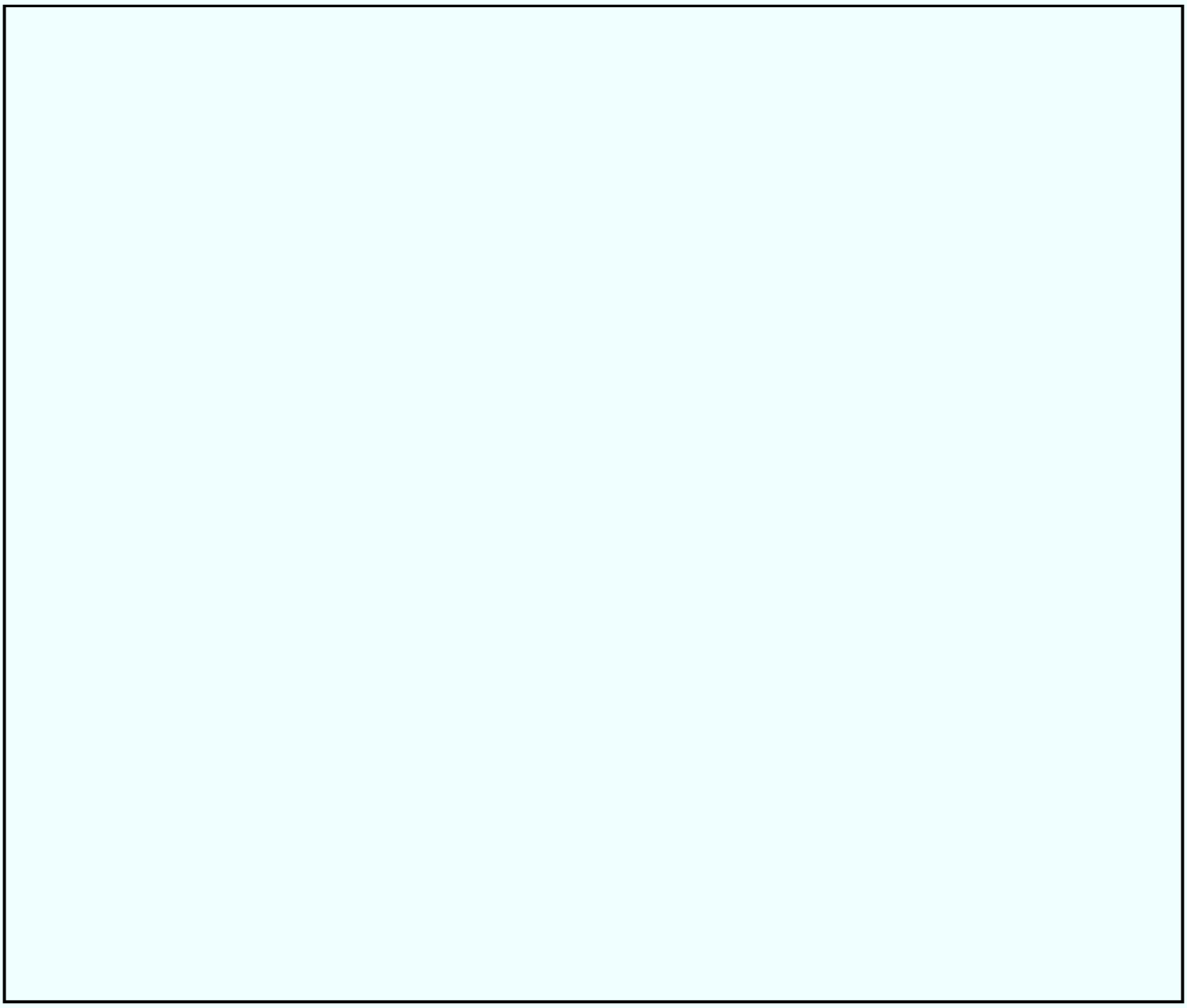


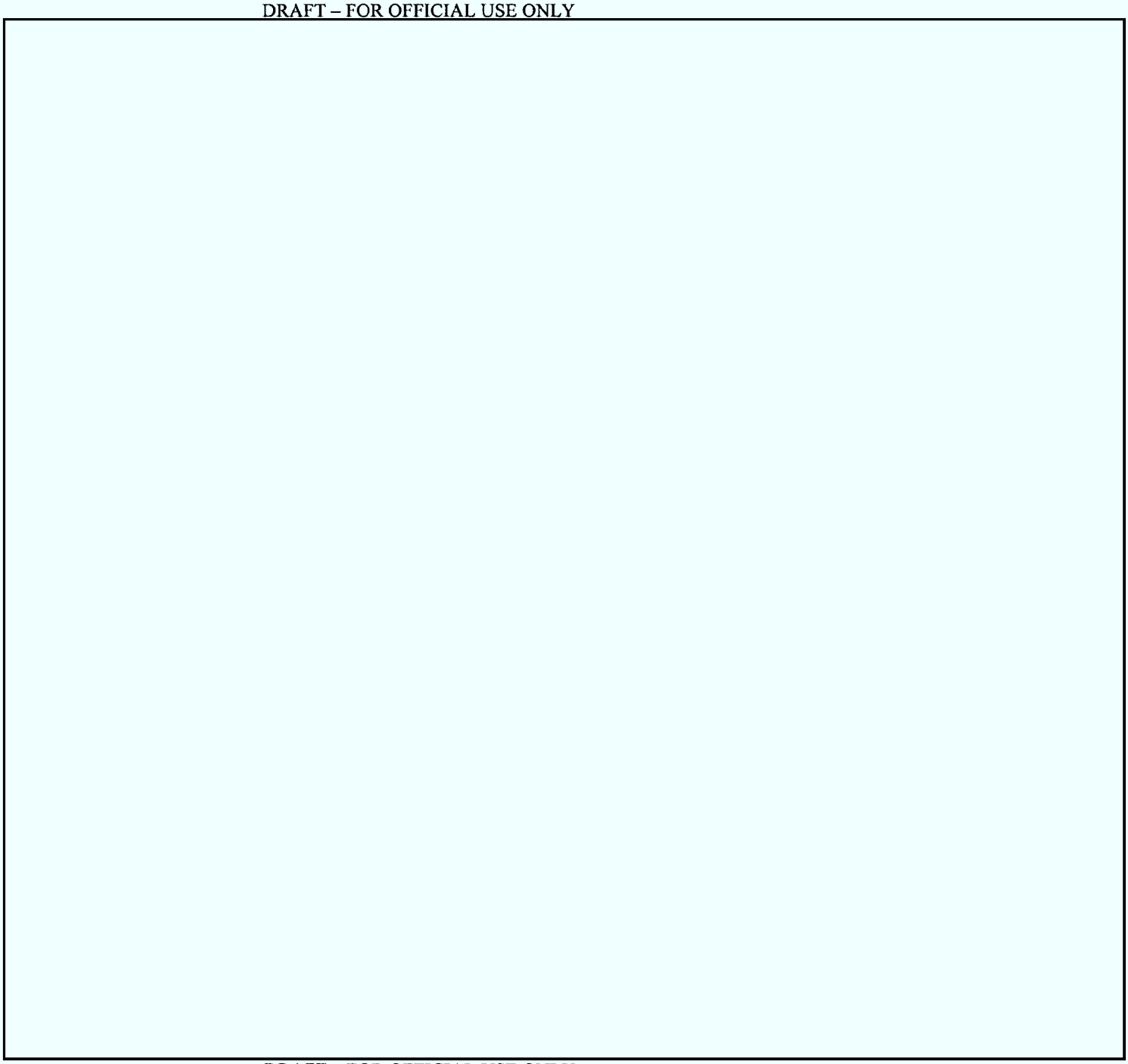
b5





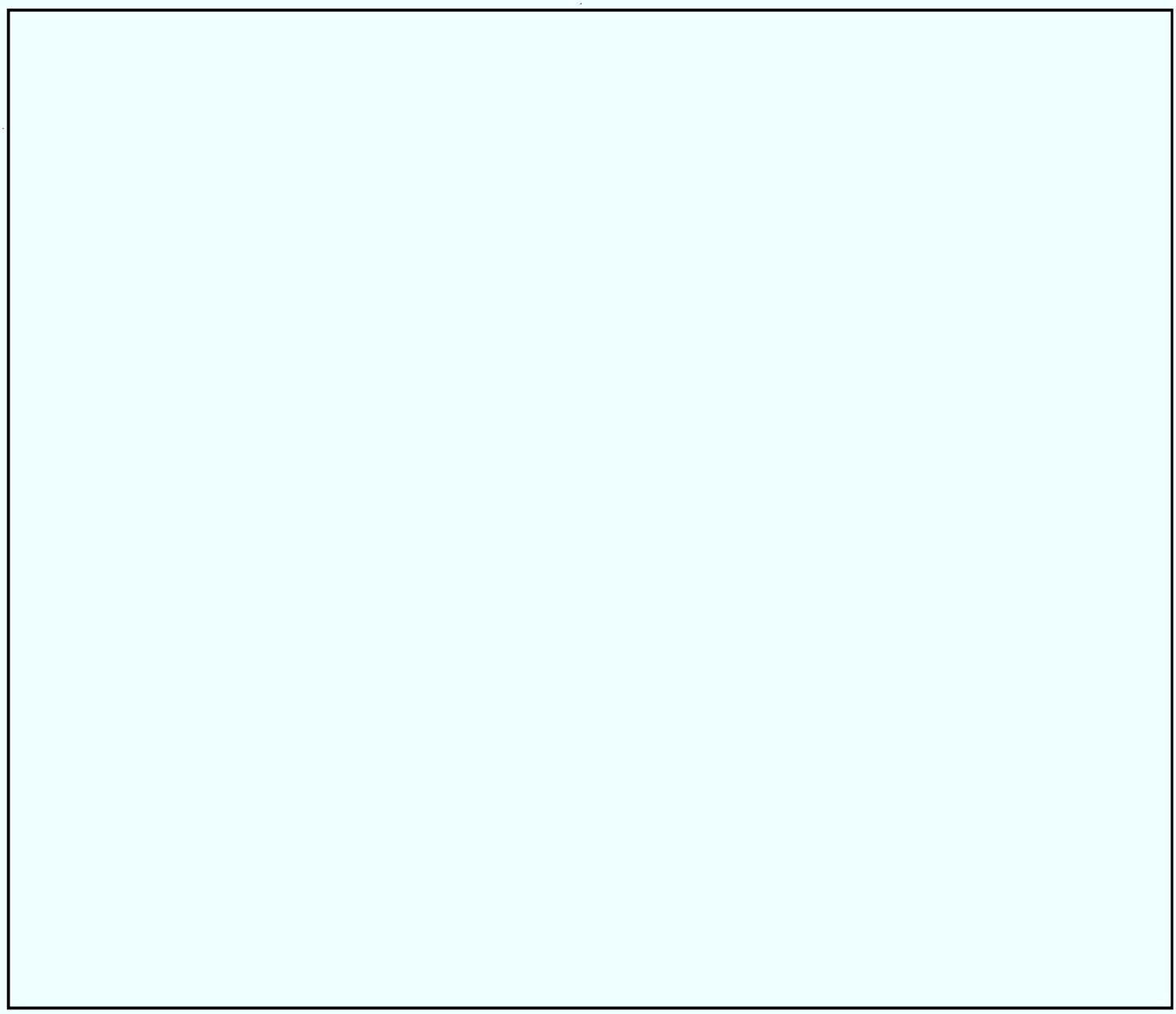
b5

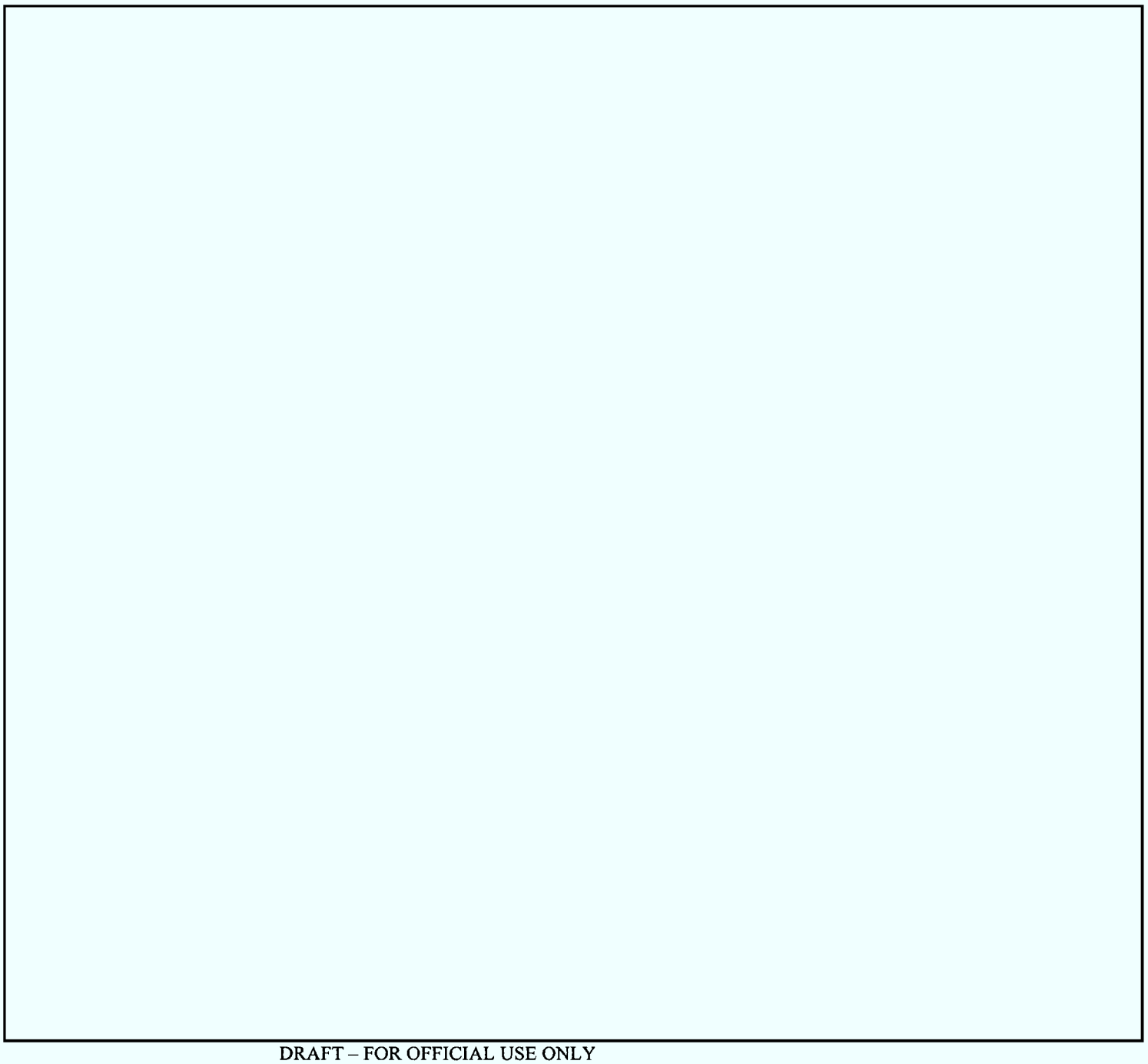




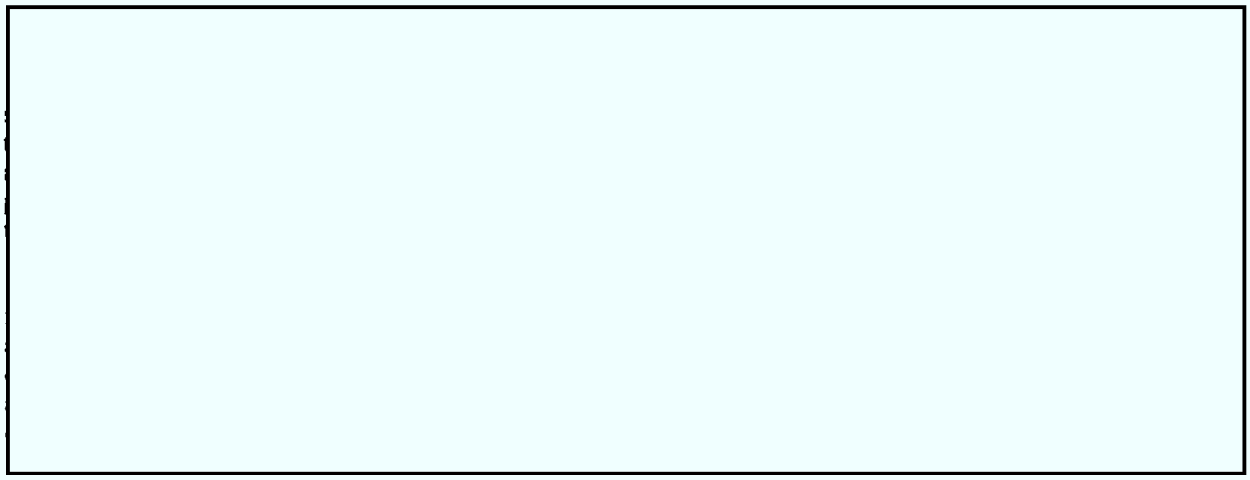
b5

b5

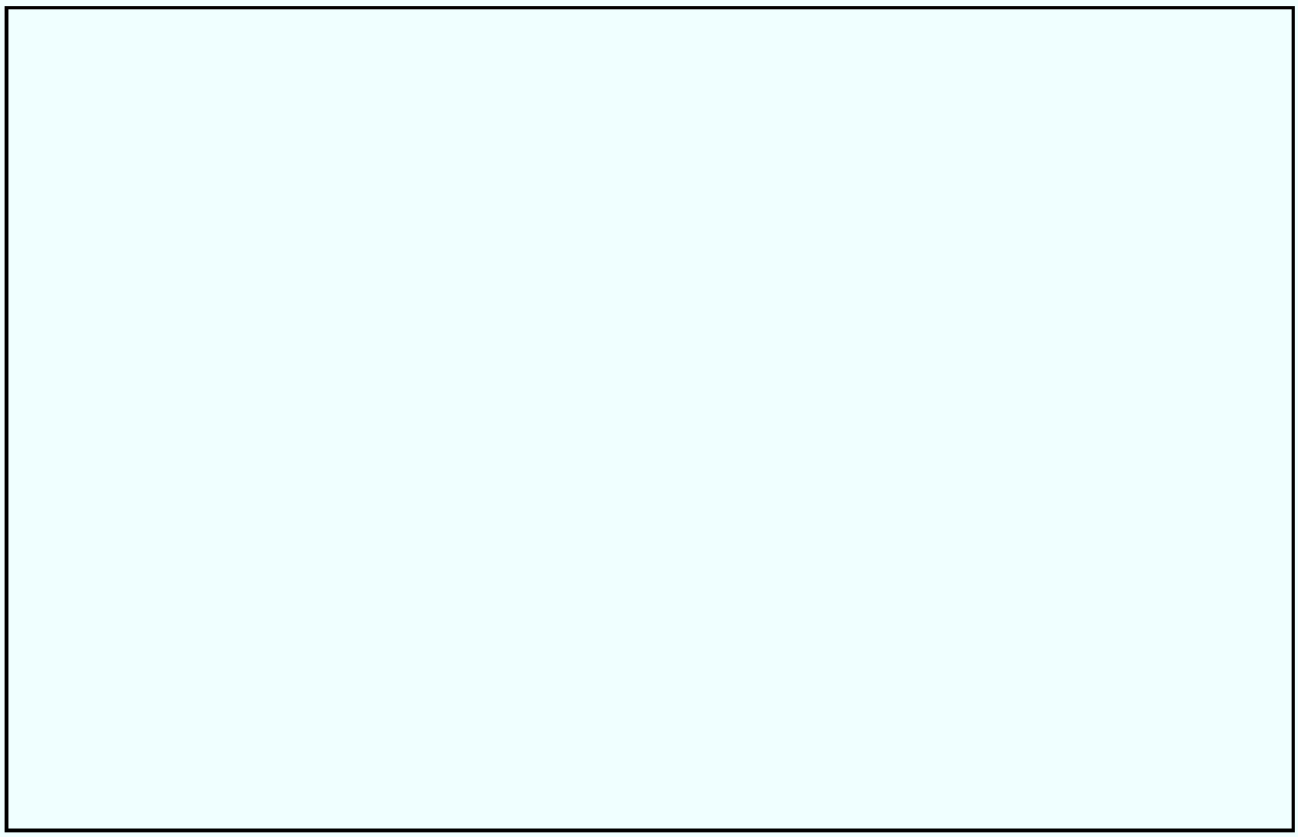




b5



PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT



PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

DRAFT: 4/19/04

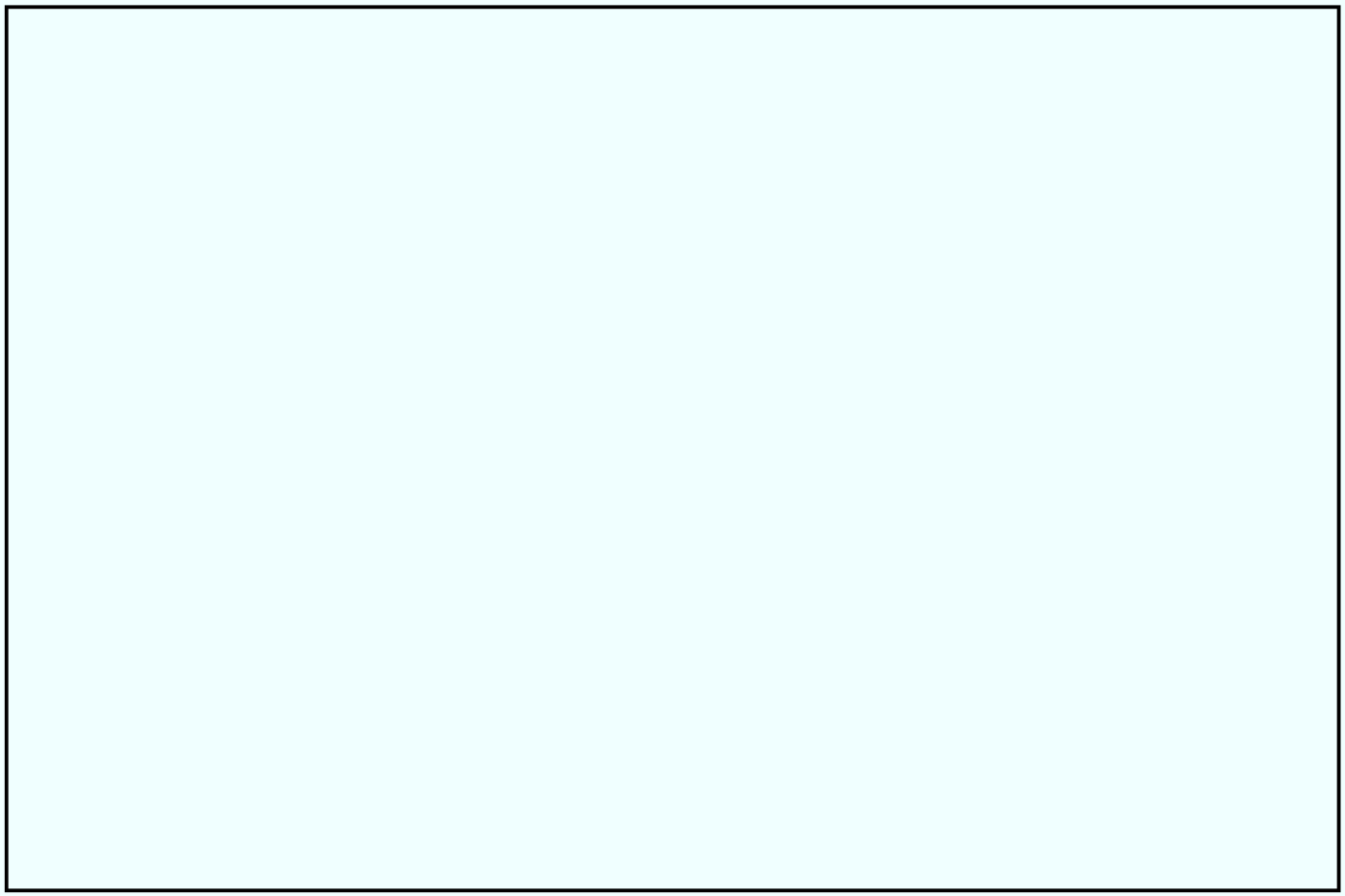
~~DATE: 10/03-2005~~ (C)
CLASSIFIED BY 65179 DMH/JHF 05-CV-0845
REASON: 1.4 (C)
DECLASSIFY ON: 10-12-2030

b5

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

DATE: 12-05-2005
CLASSIFIED BY 65179/DMH/LP/DK
REASON: 1.4 ((C) 05-CV-0845)
DECLASSIFY ON: 12-05-2030

b5

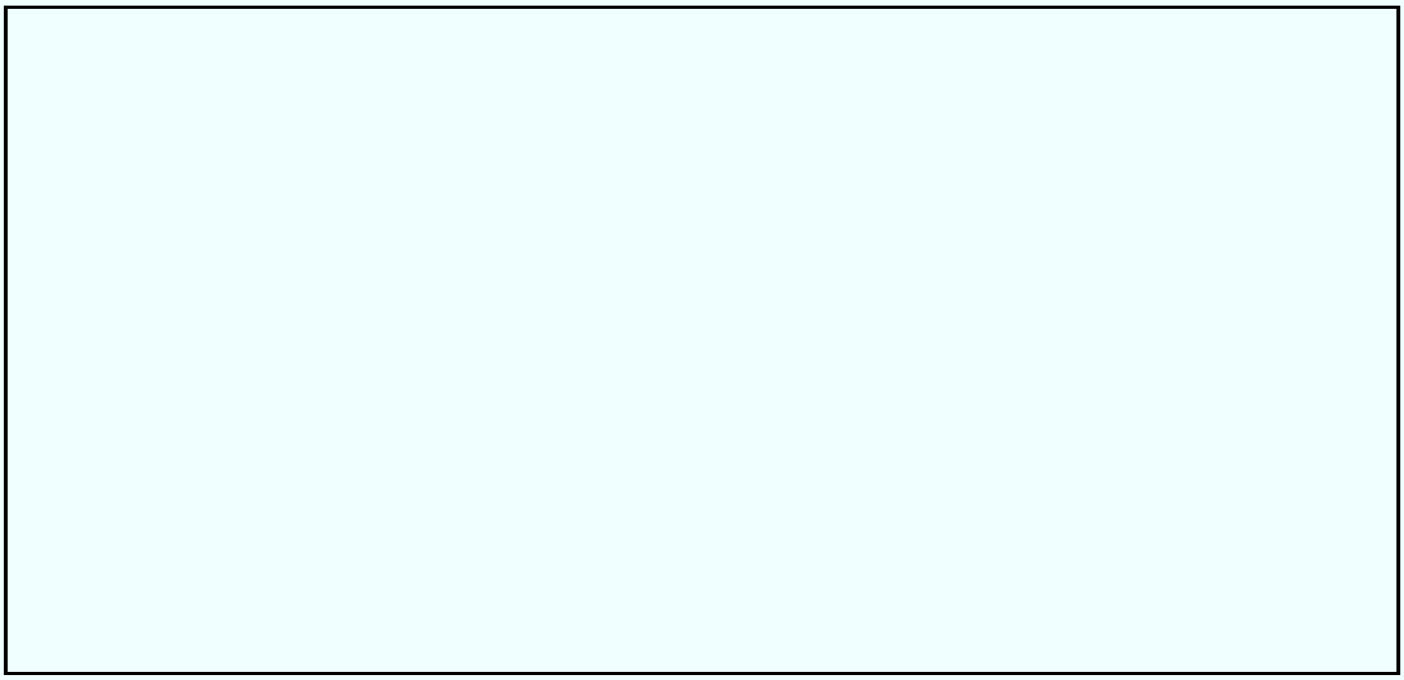


PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5

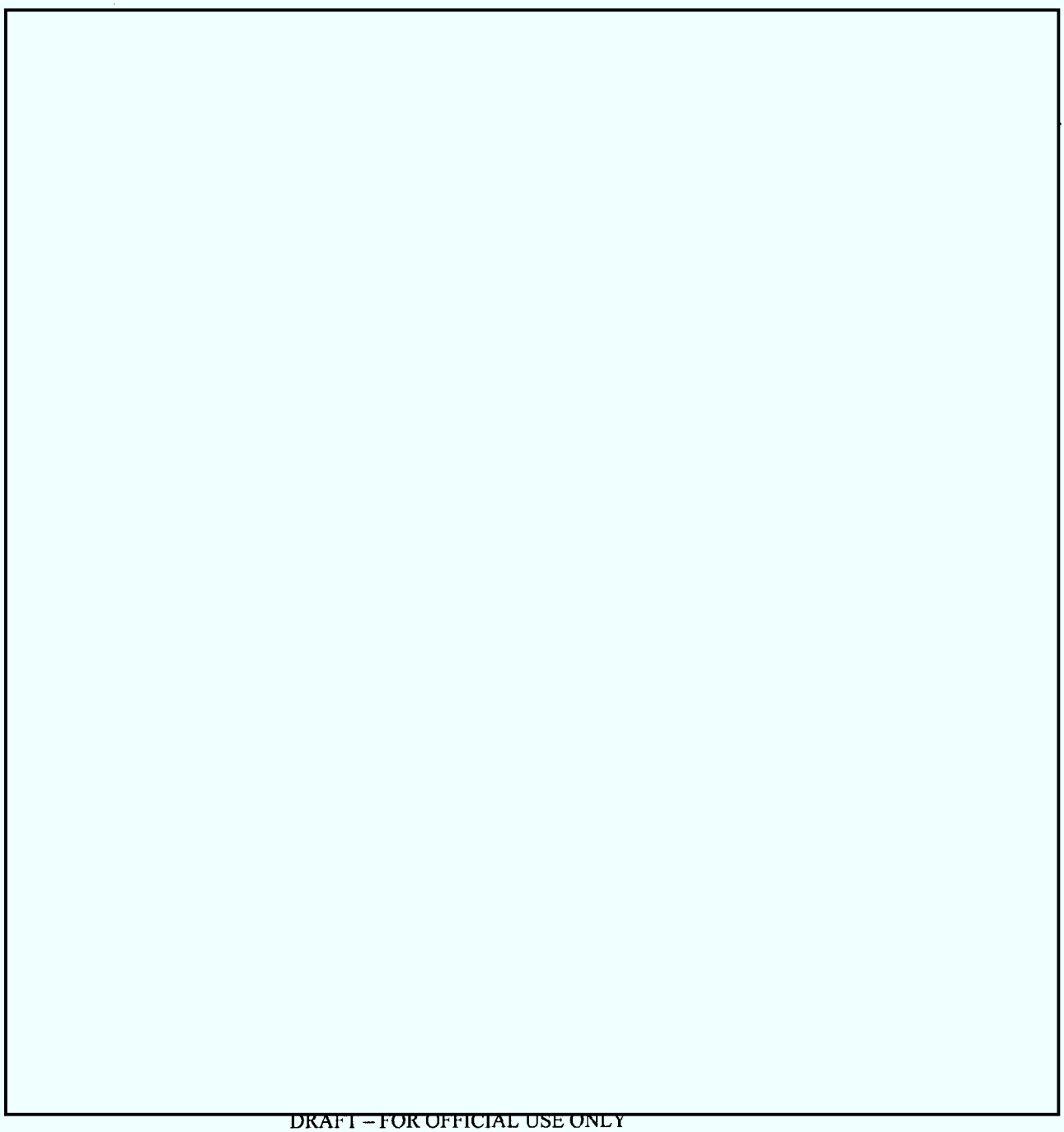
PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5



PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5

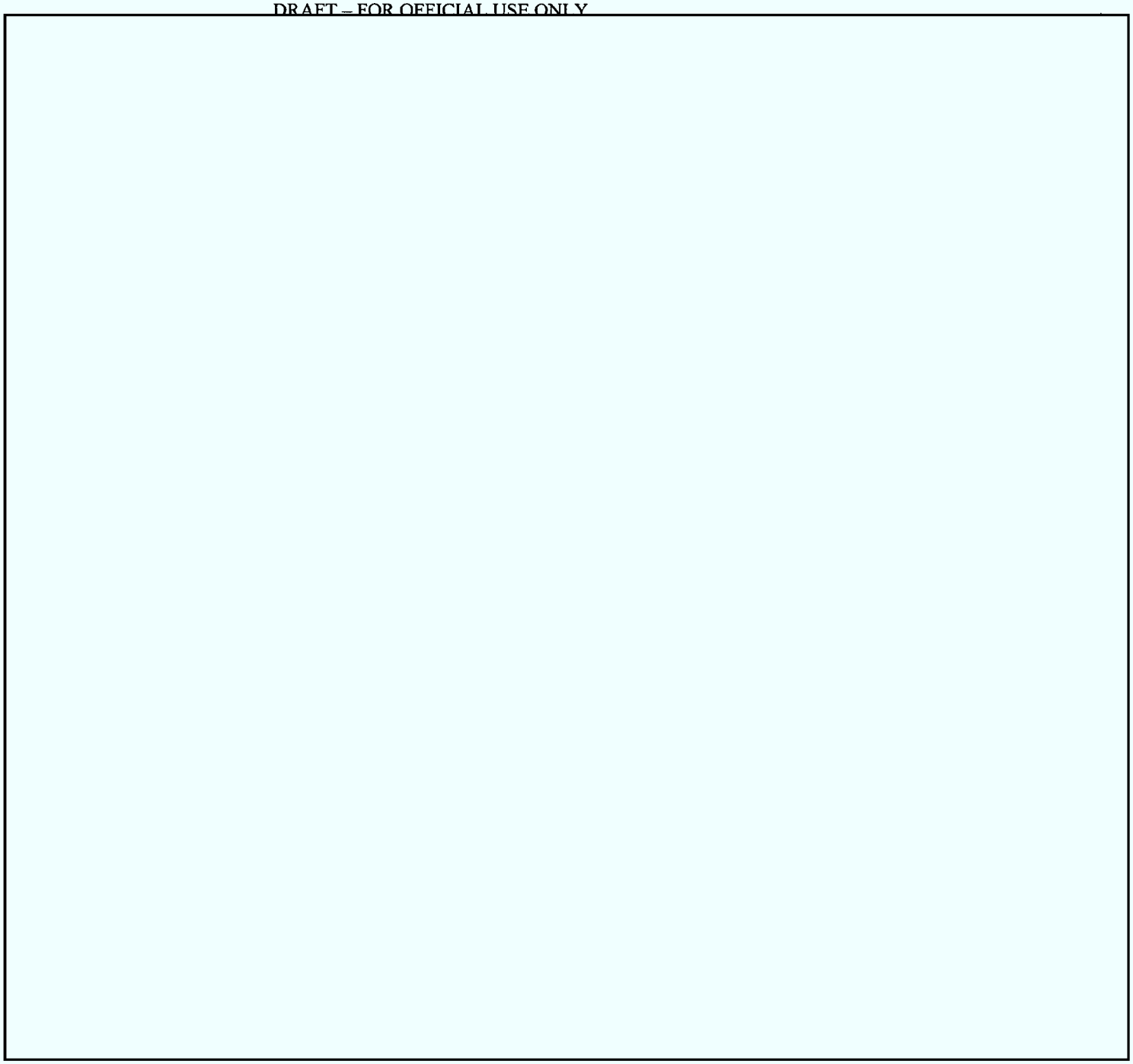


PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

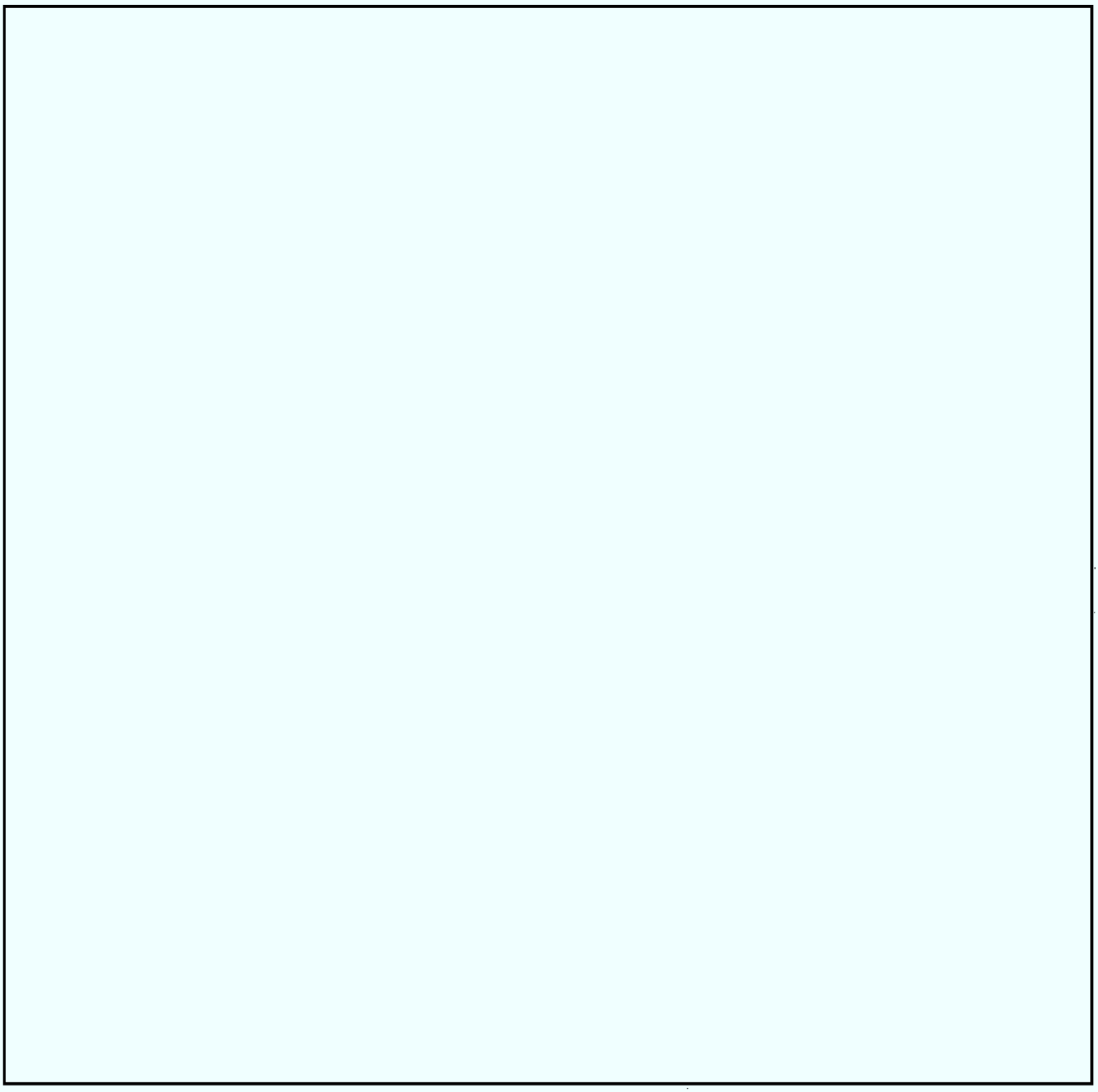
b5



PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5

DRAFT – FOR OFFICIAL USE ONLY



DRAFT – FOR OFFICIAL USE ONLY

SECRET

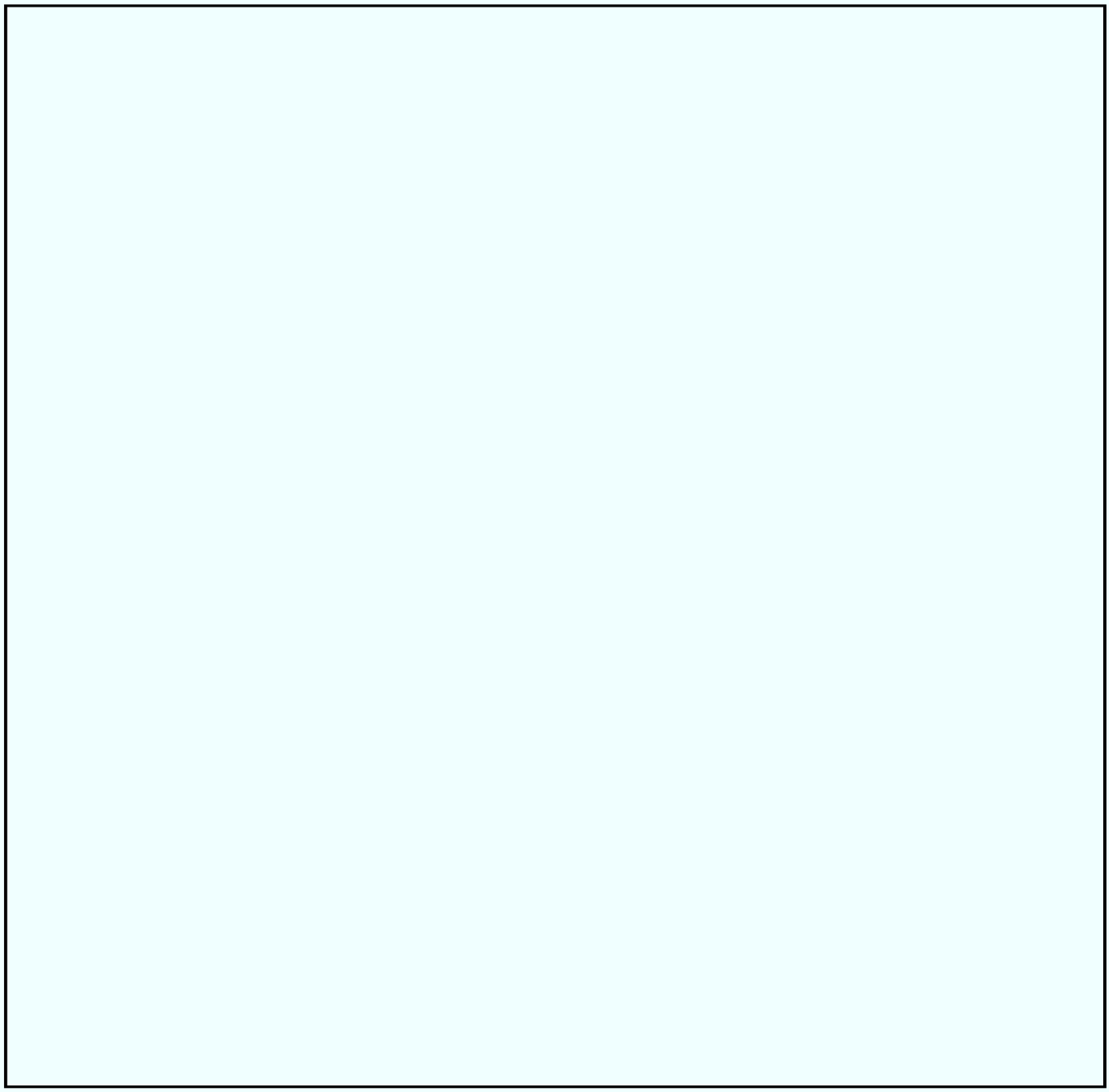
PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5

[redacted]

b5

[redacted]



b5

b5

b5

b5

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5

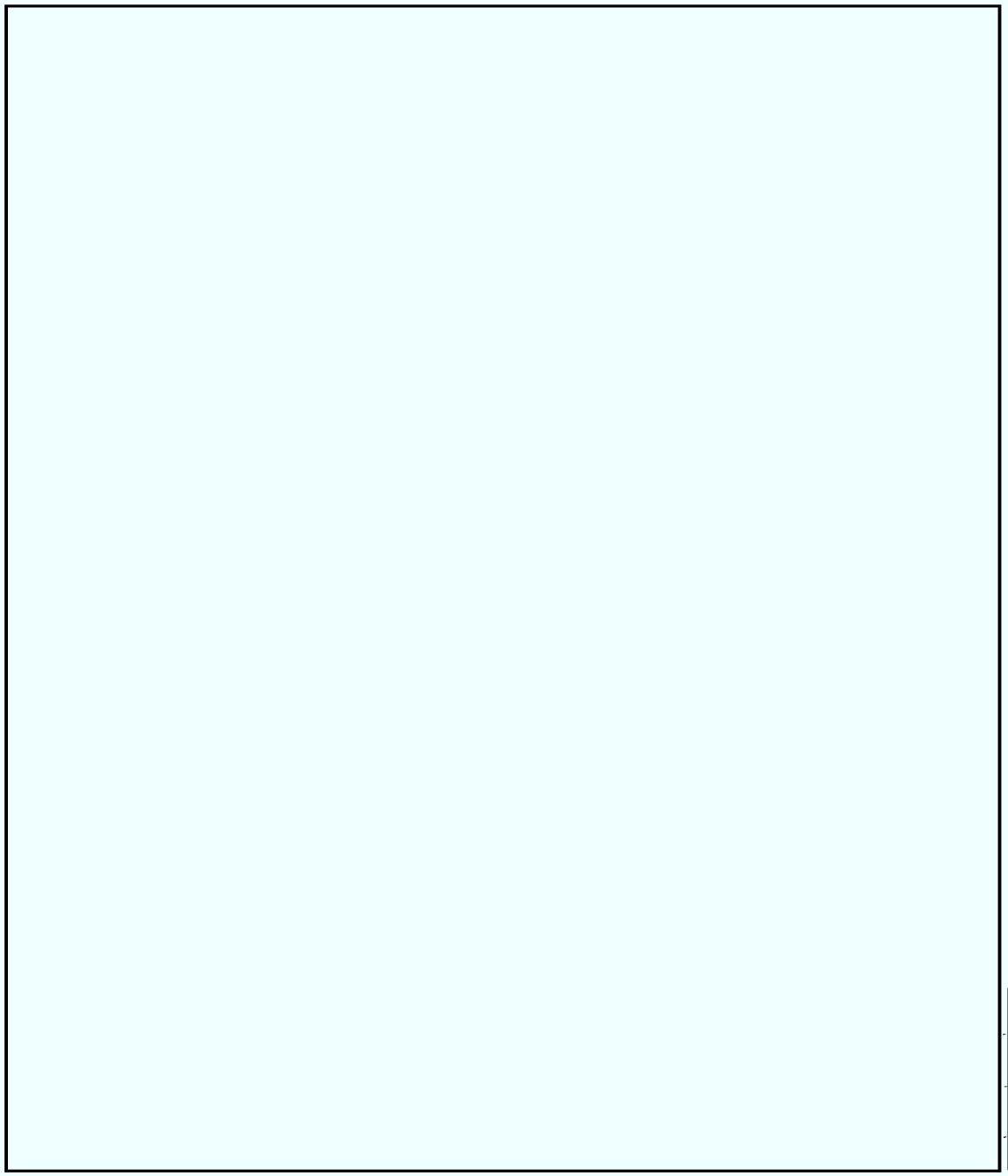
[redacted]

b5

[redacted]

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

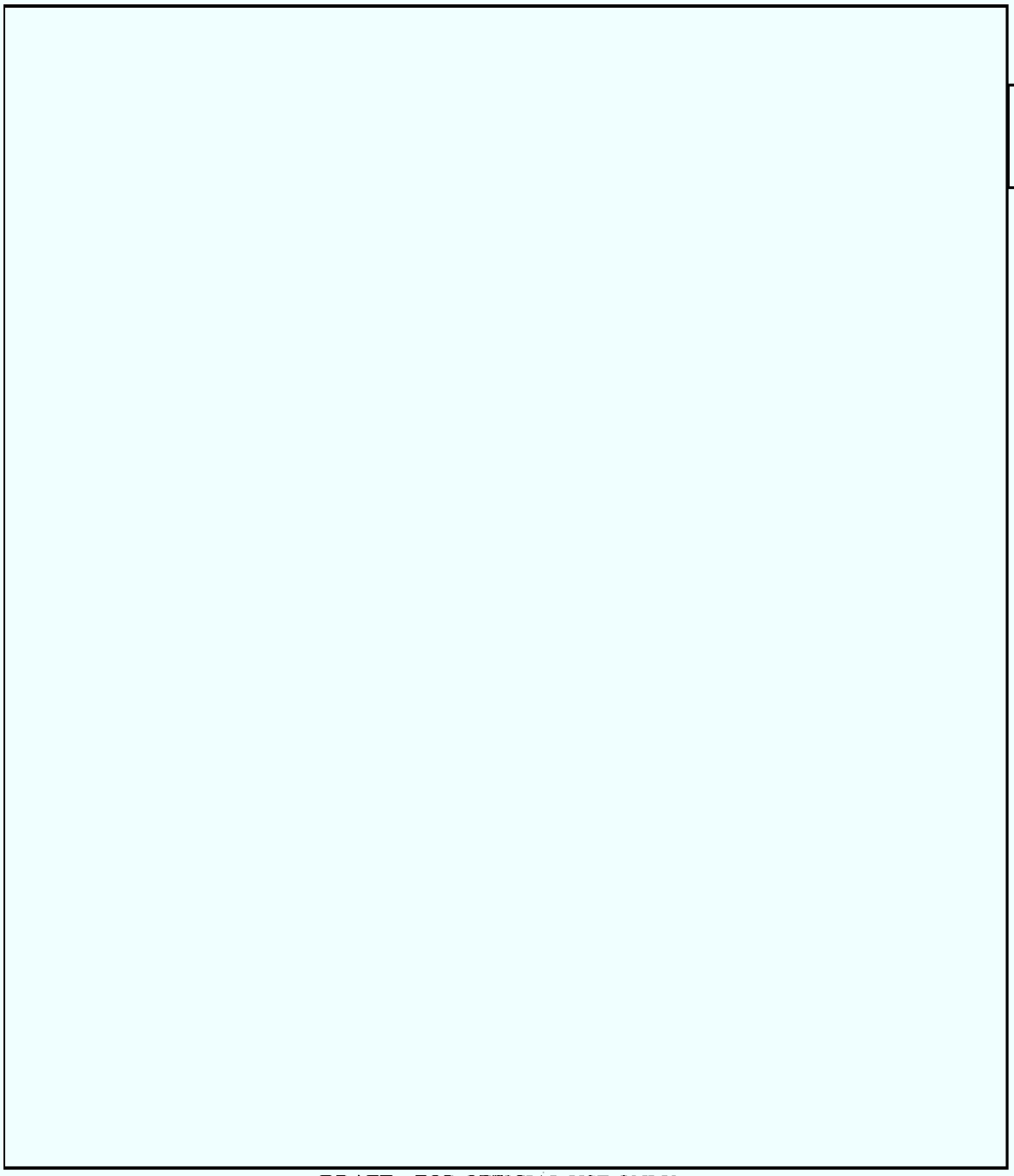
b5



b5

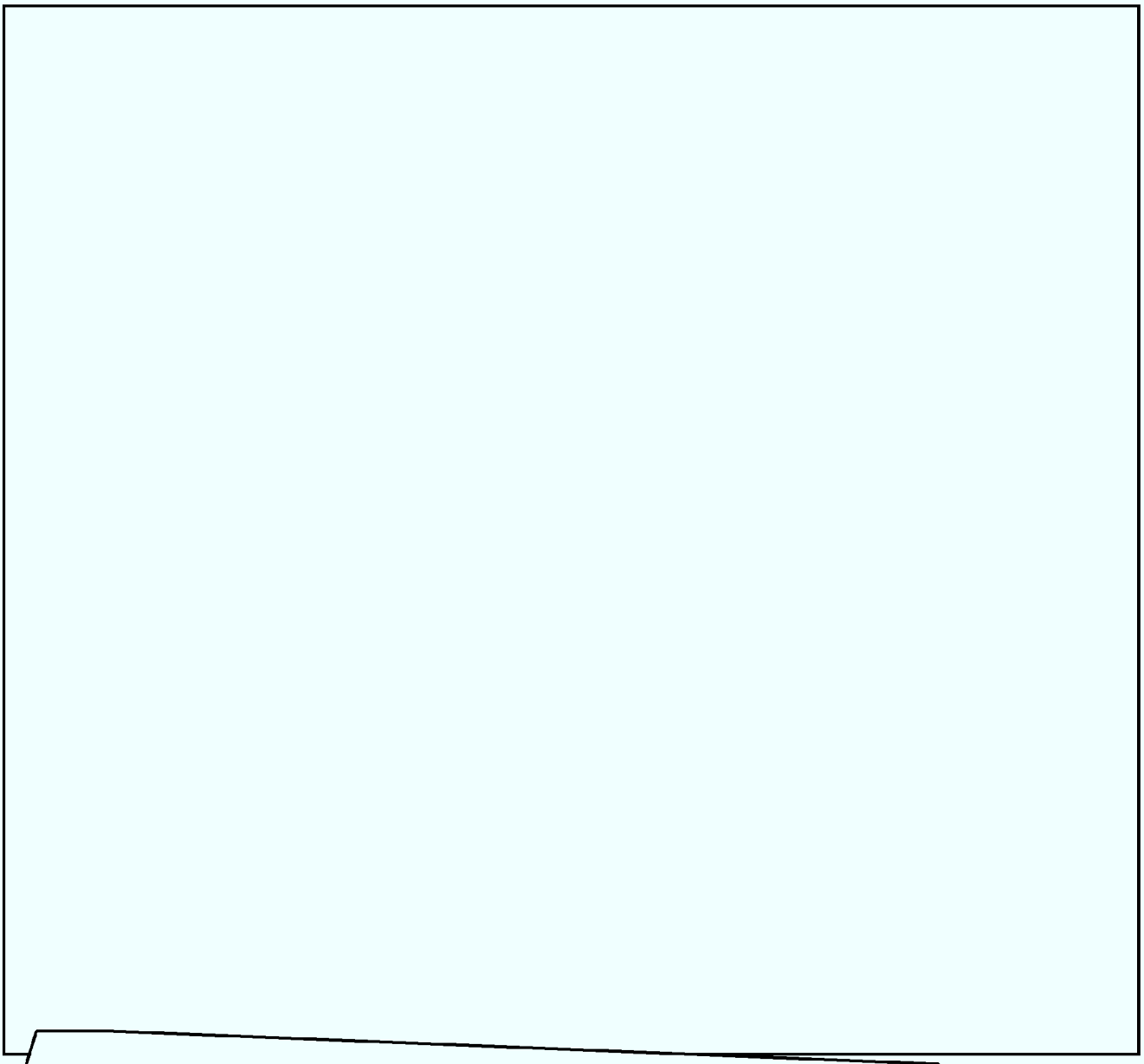
PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5



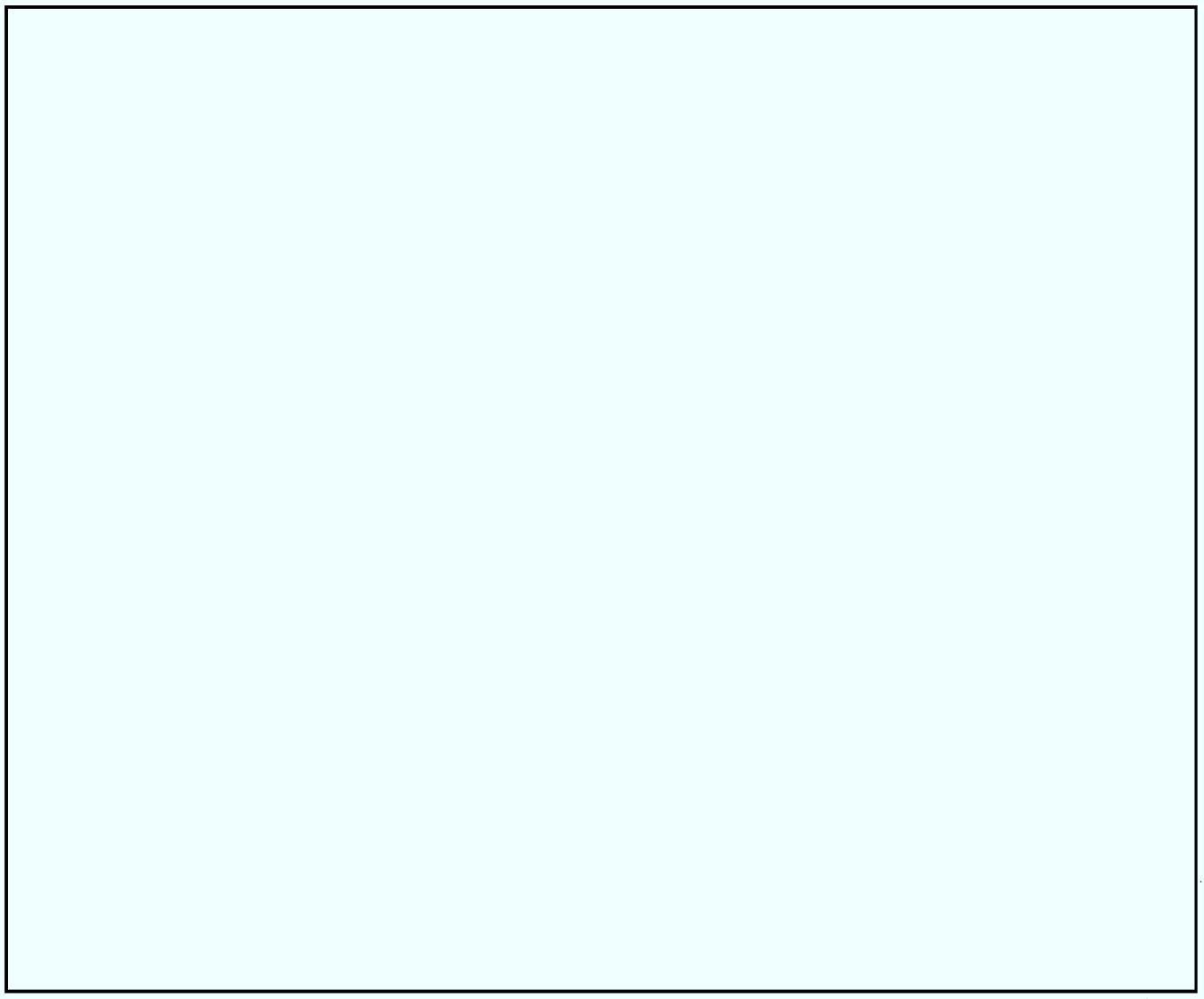
b5

b5



PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5

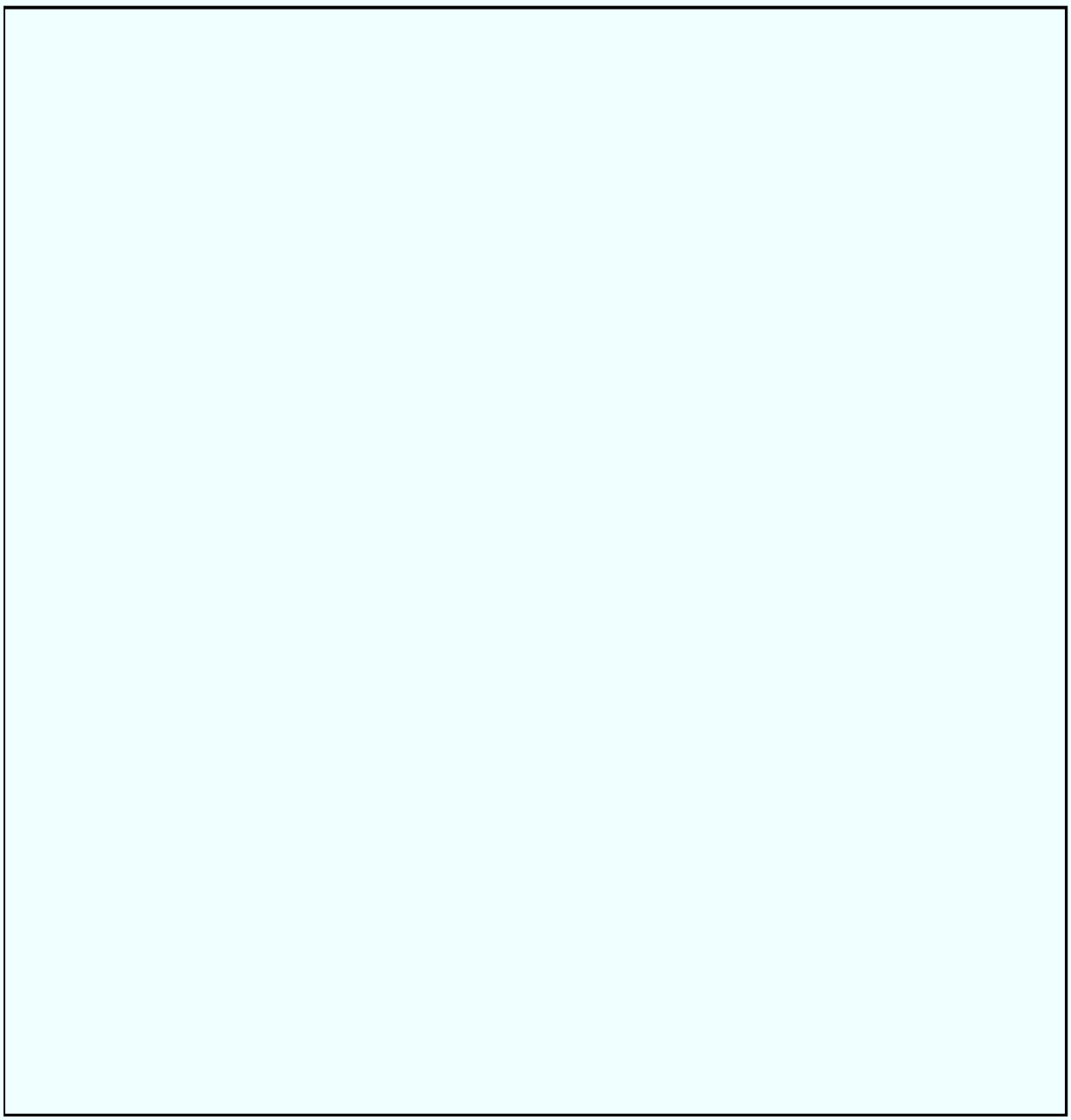


PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5

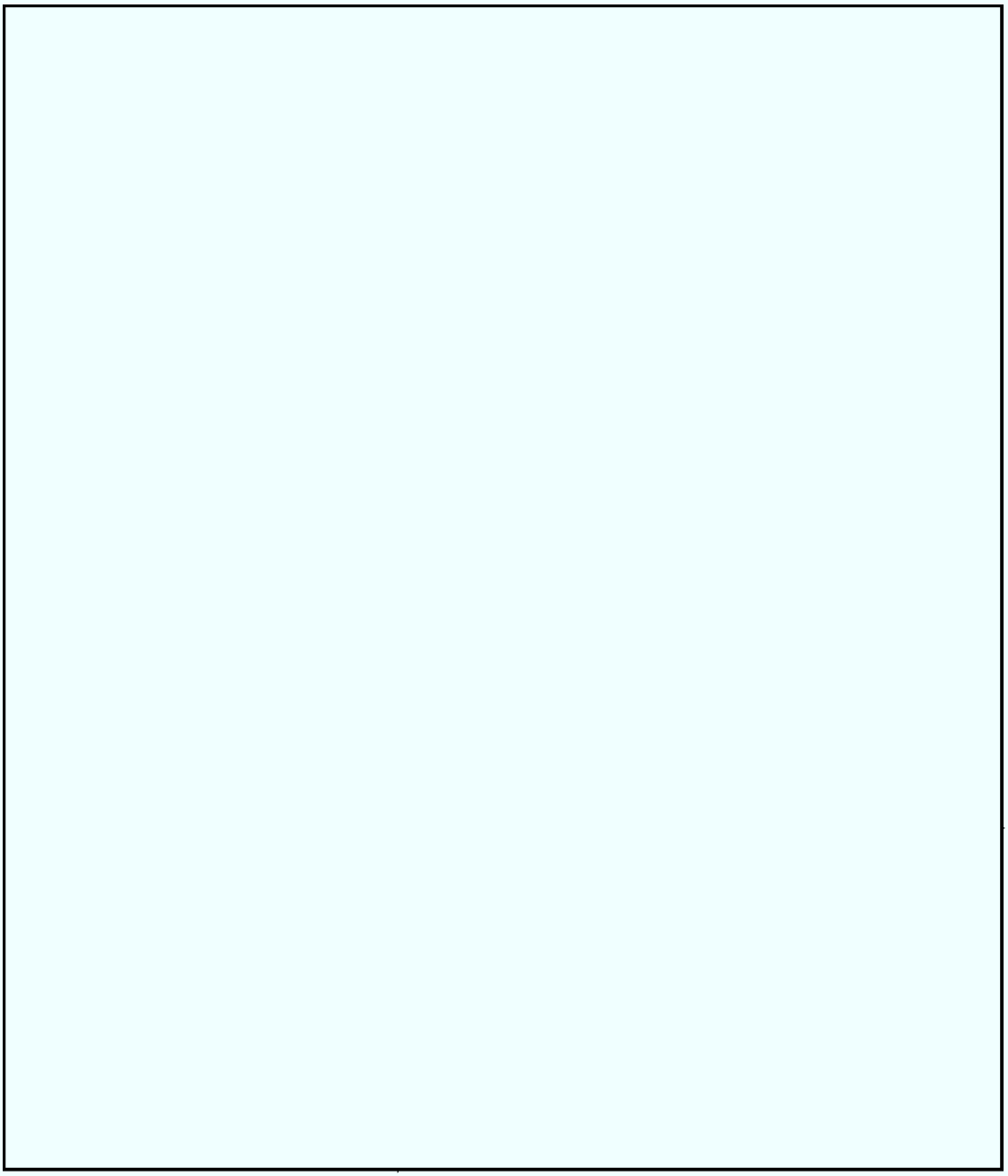
b5

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT



PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

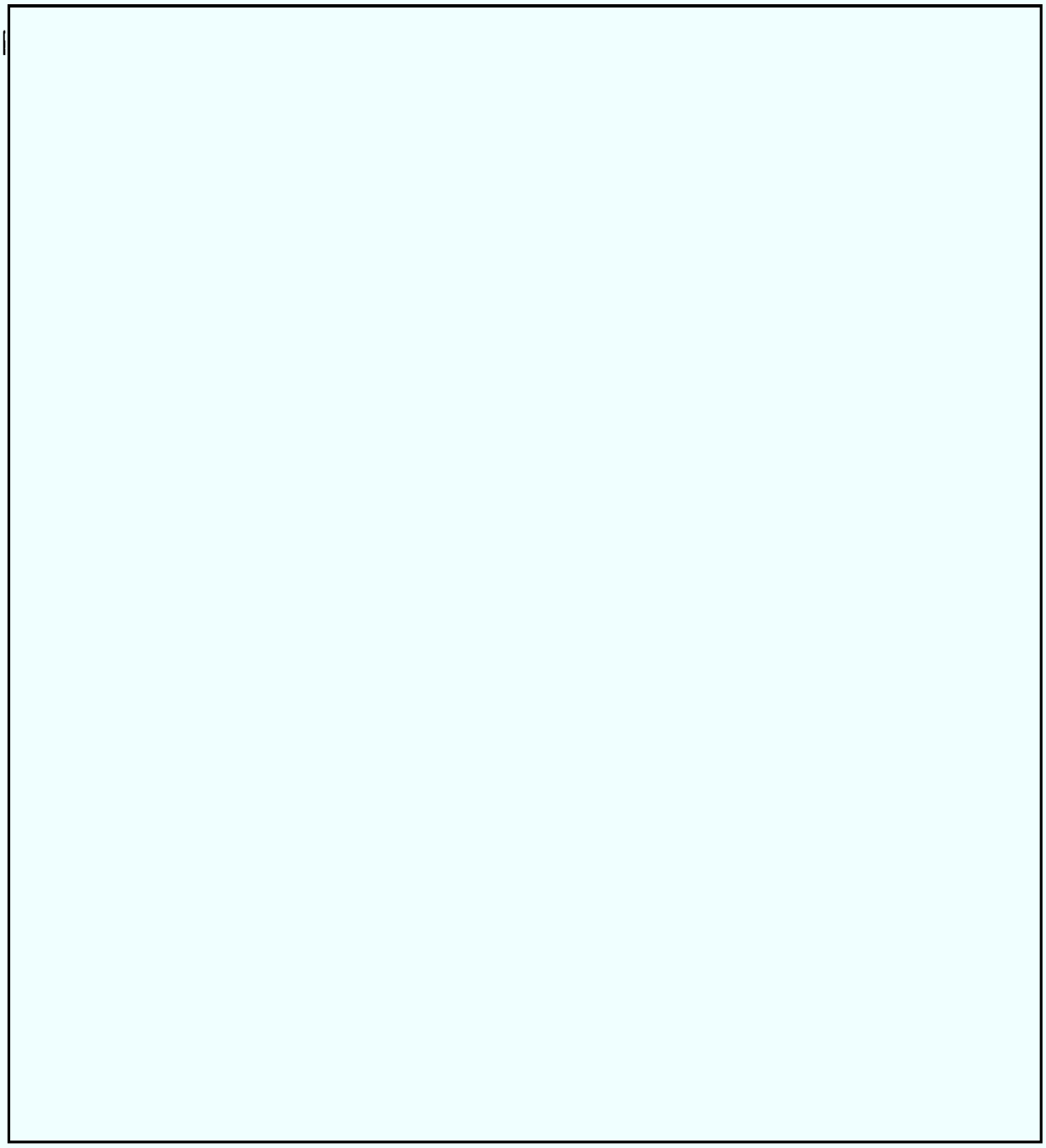
b5



b5

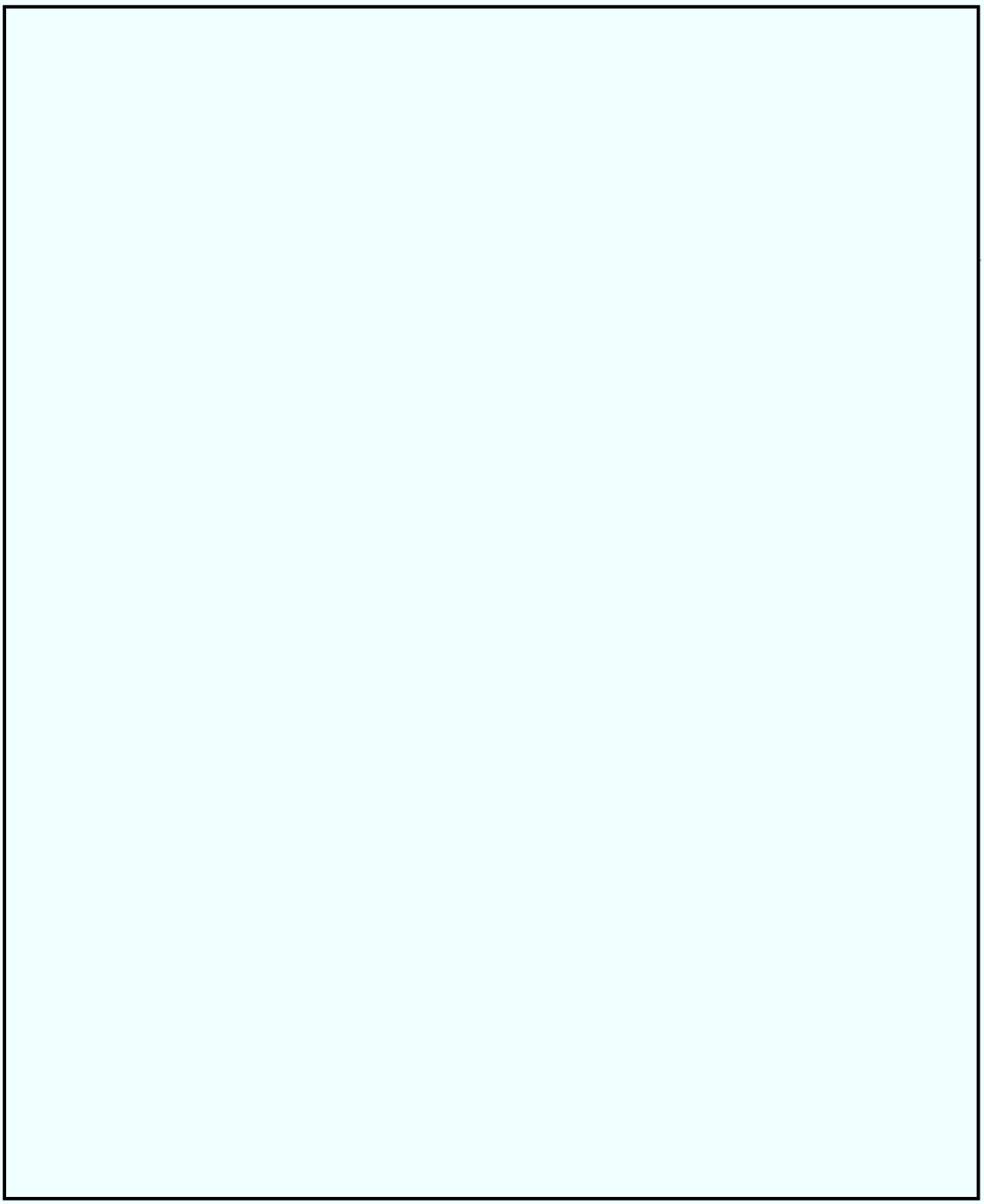
b5

b5



PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5

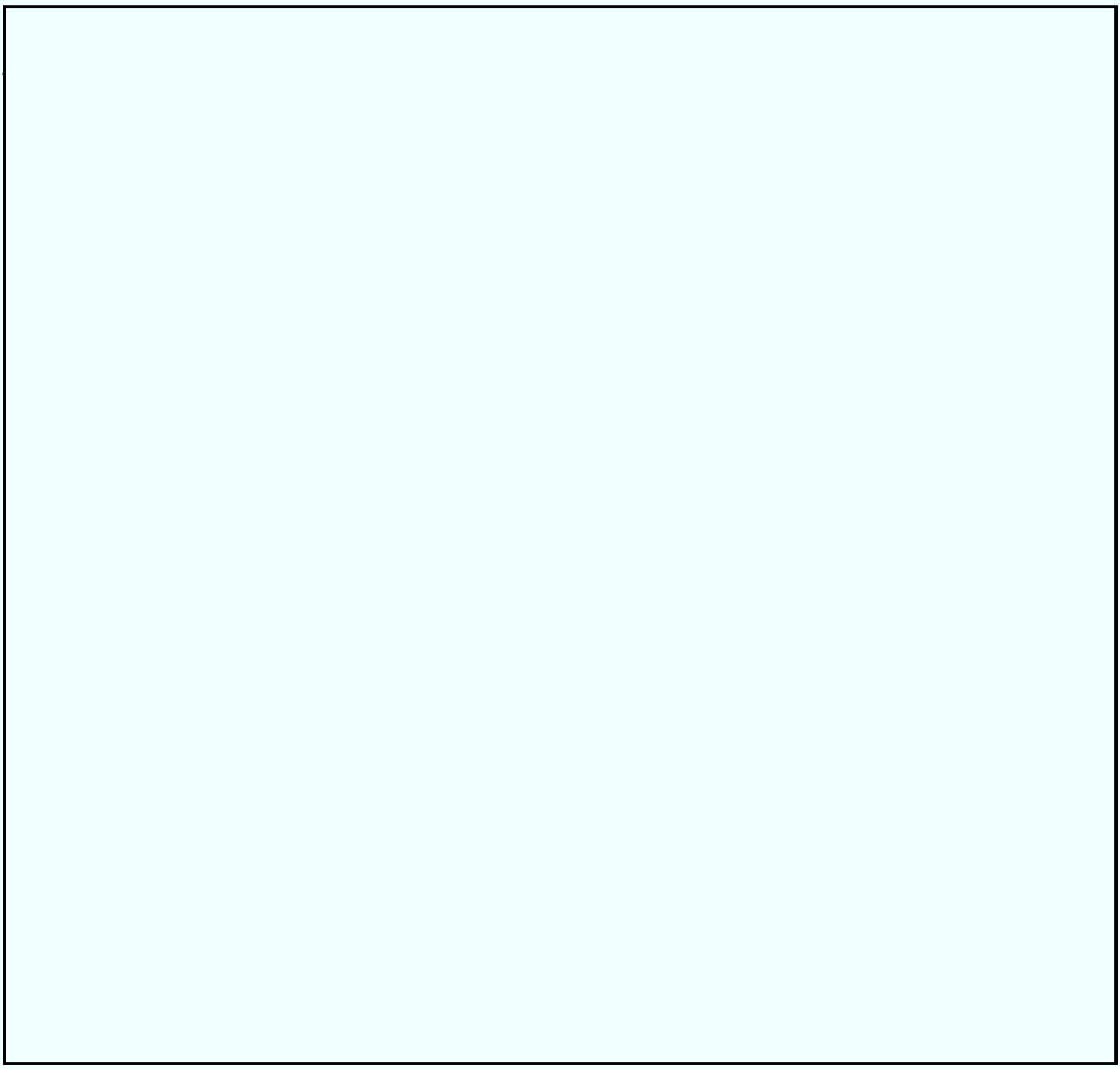


b5

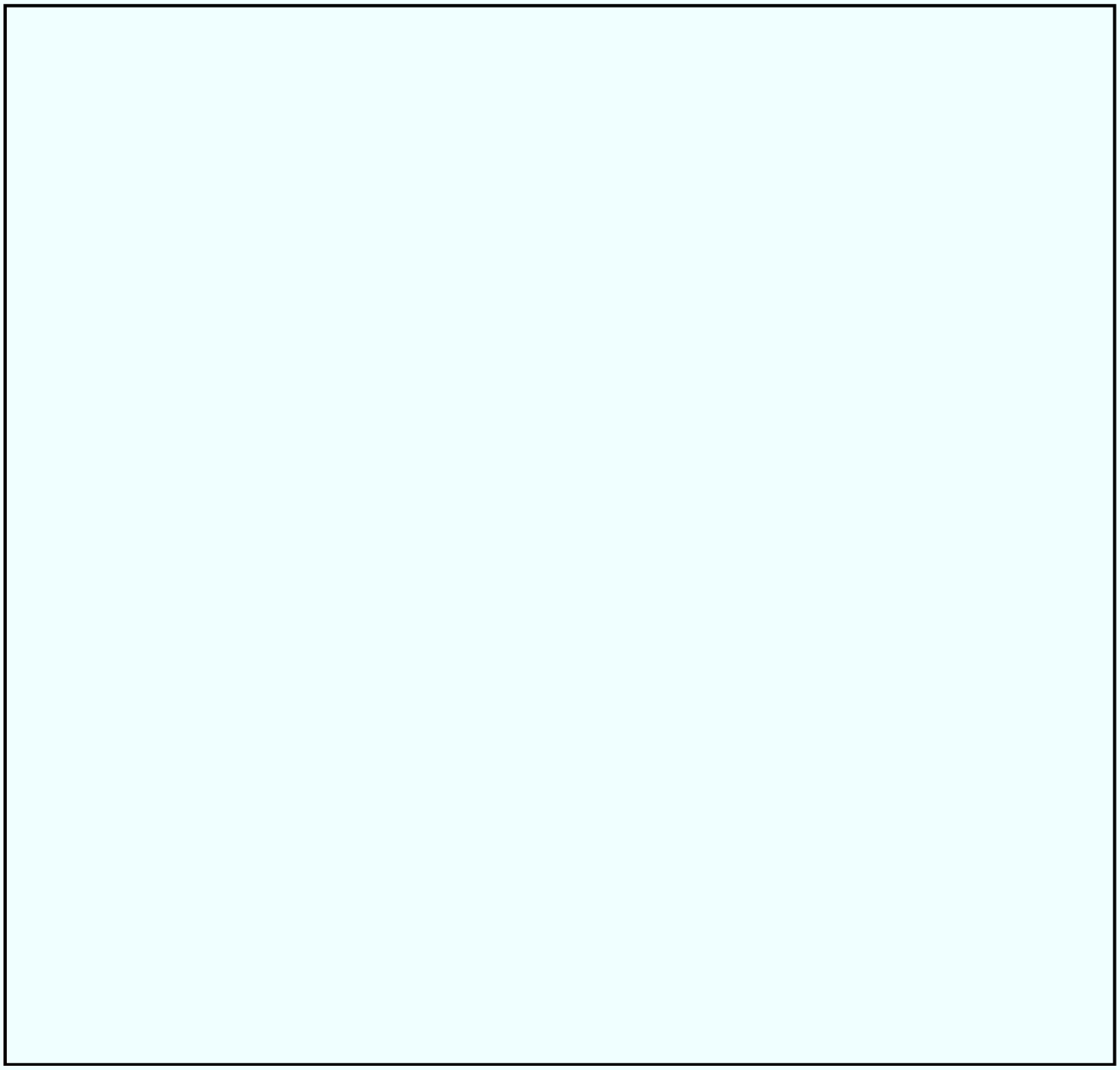
PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

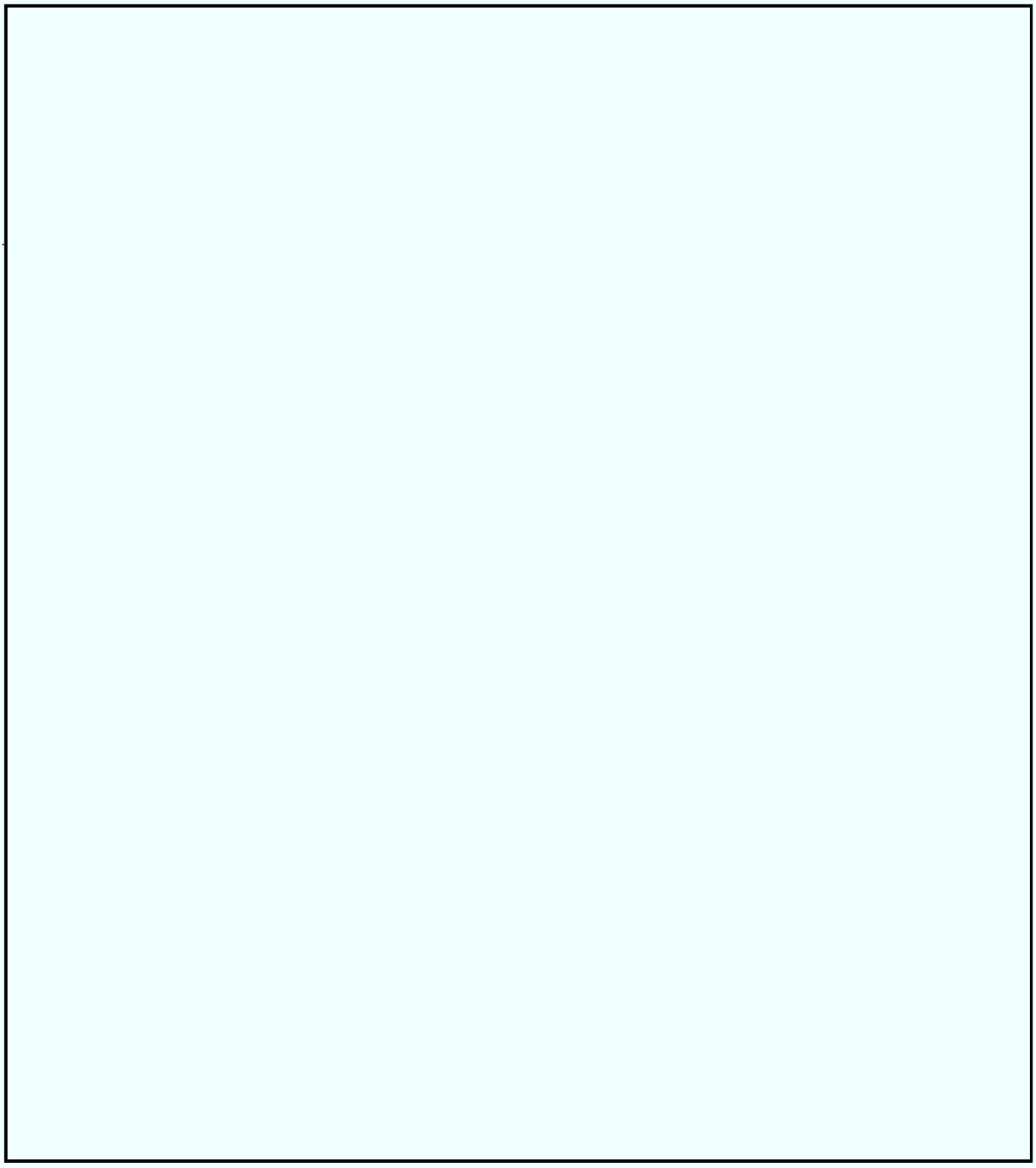


b5



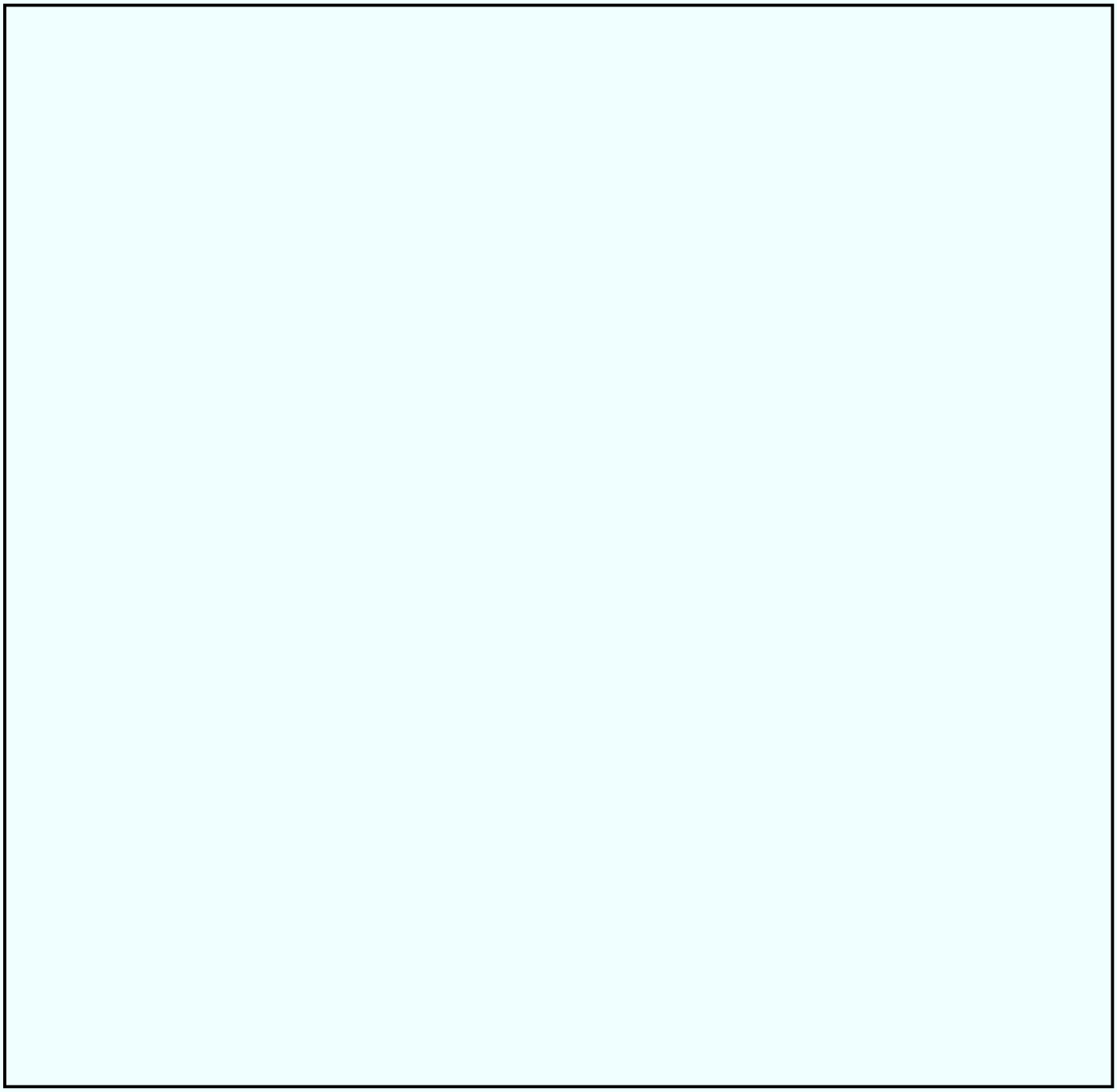
PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5



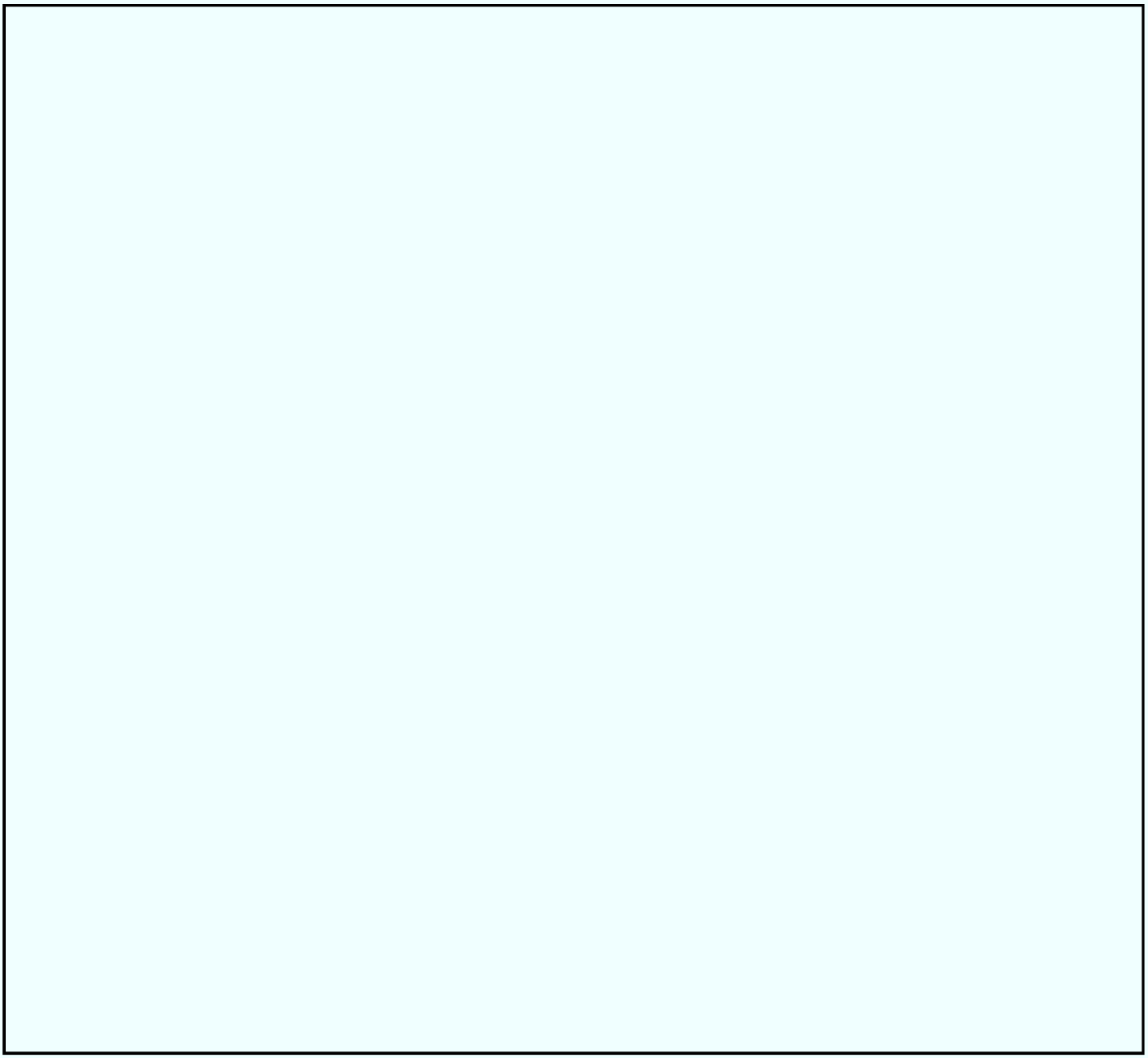
PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5



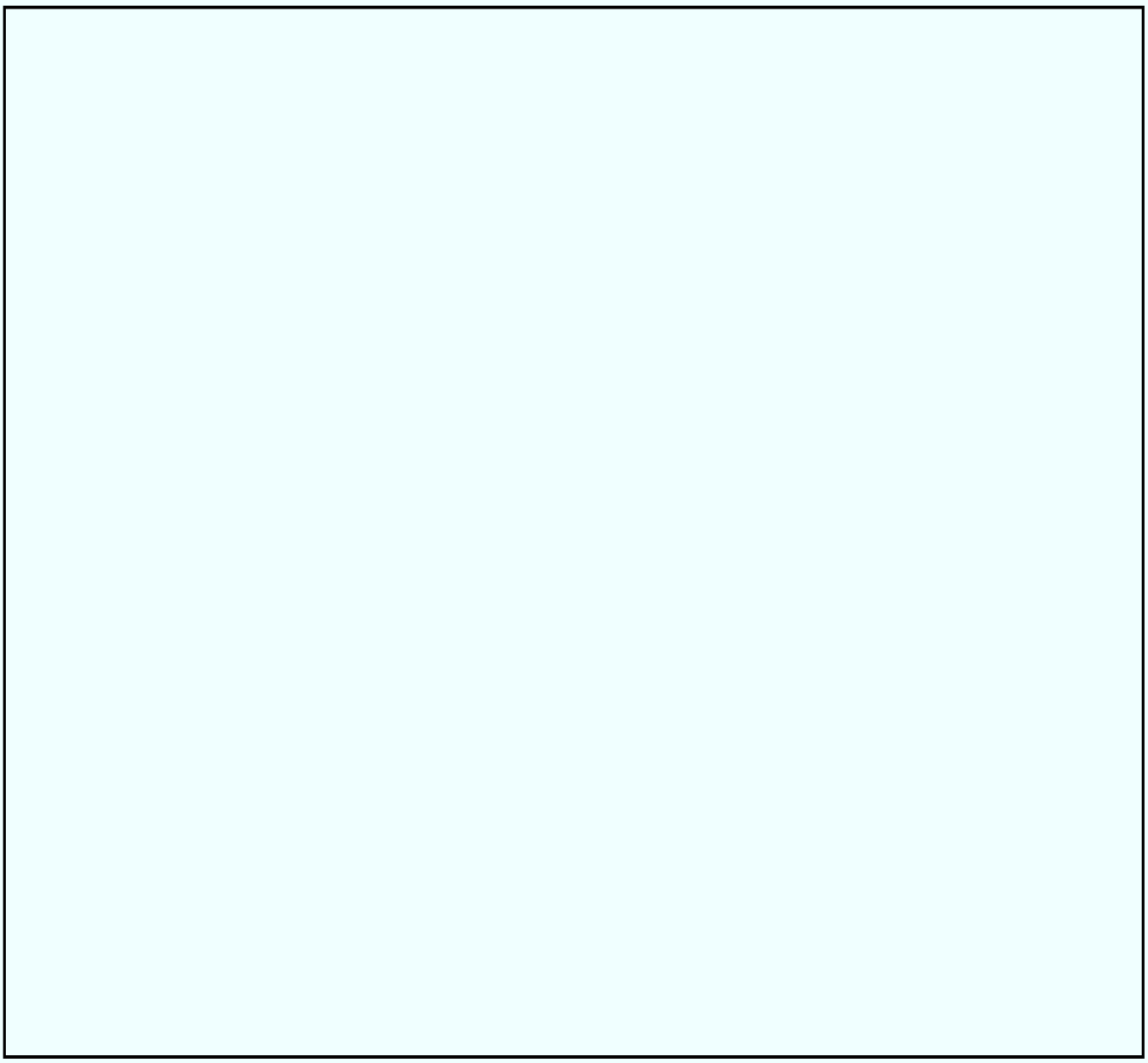
PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5



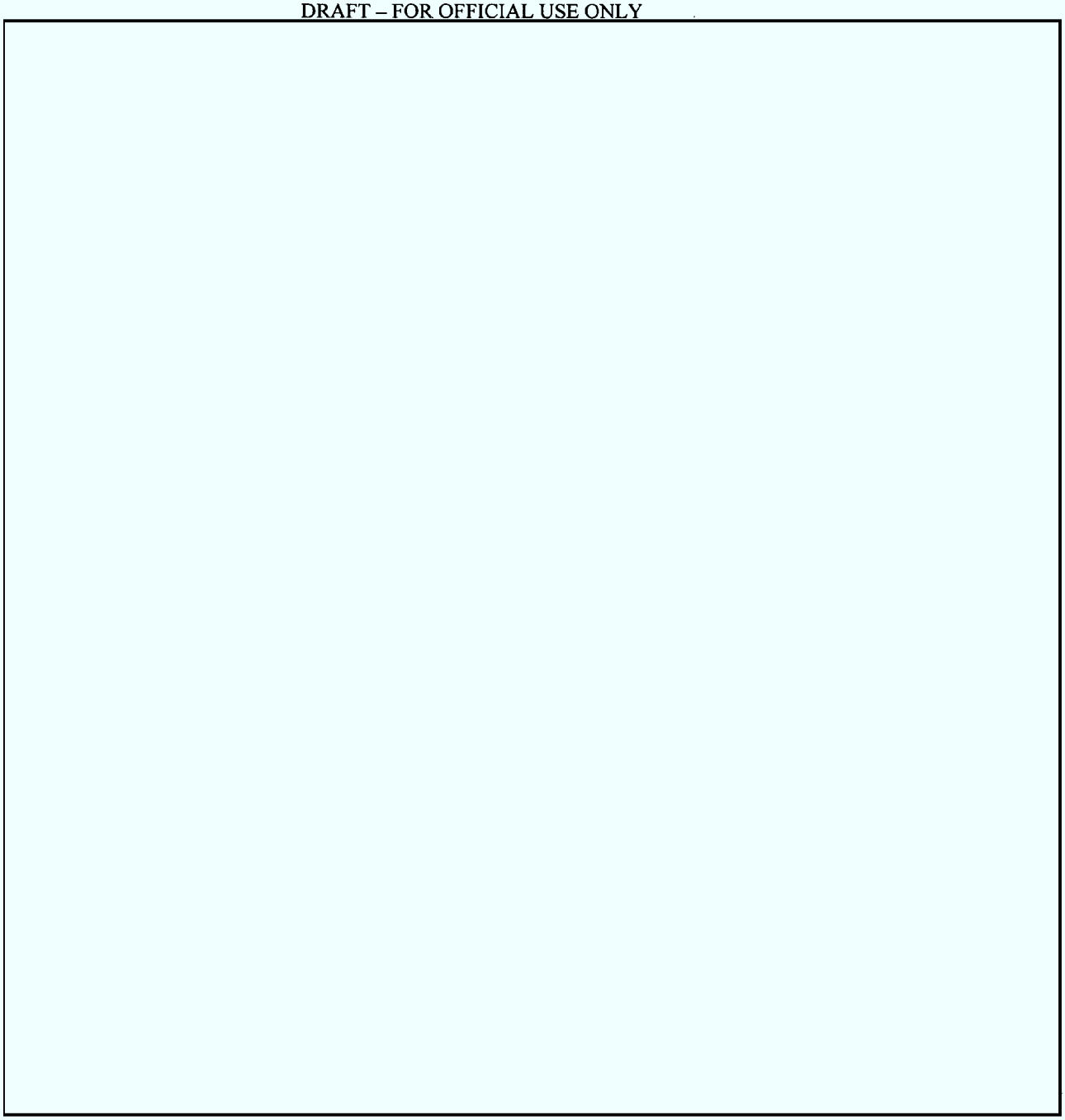
PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5



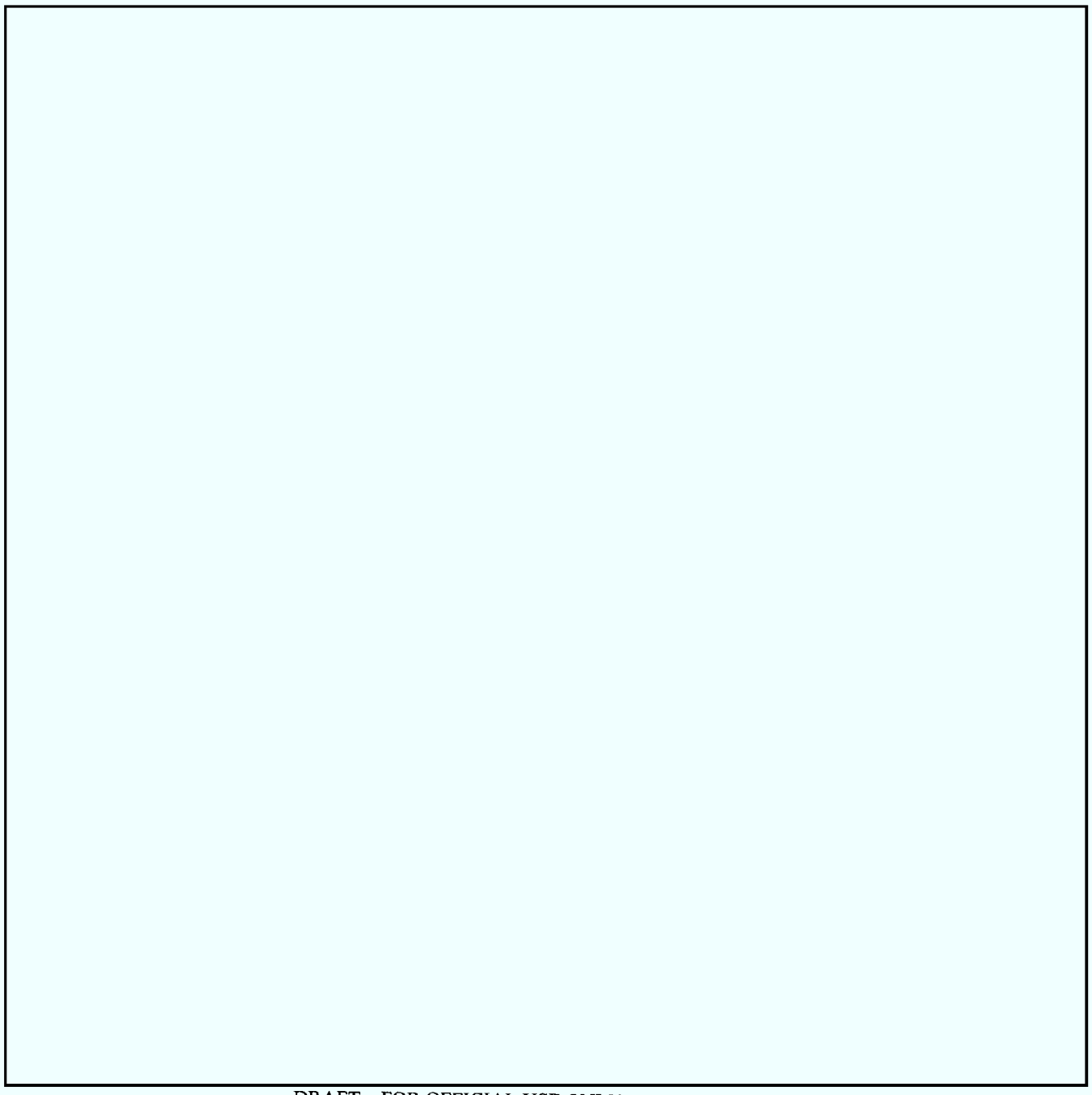
PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5



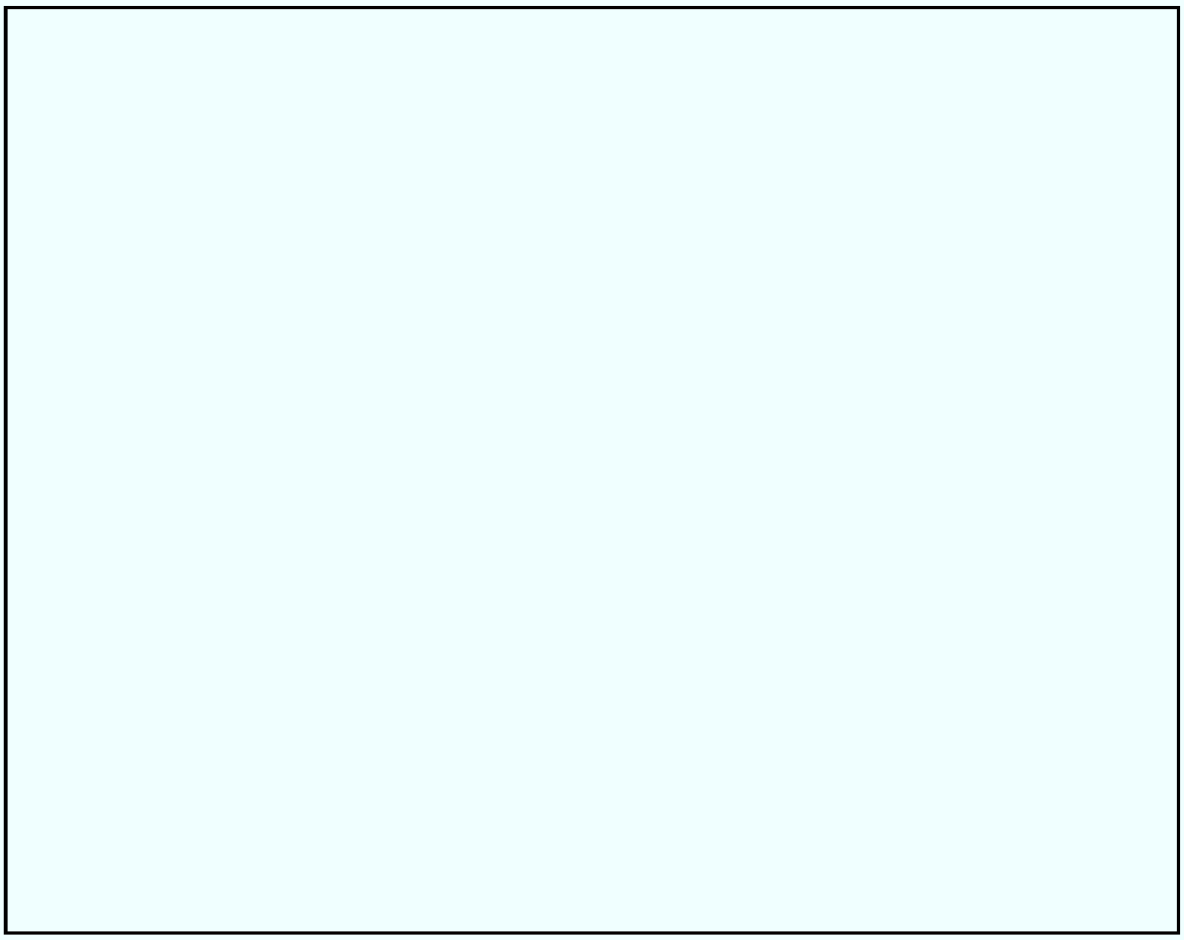
PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5



PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5



PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

[redacted] b5

[redacted] (S)

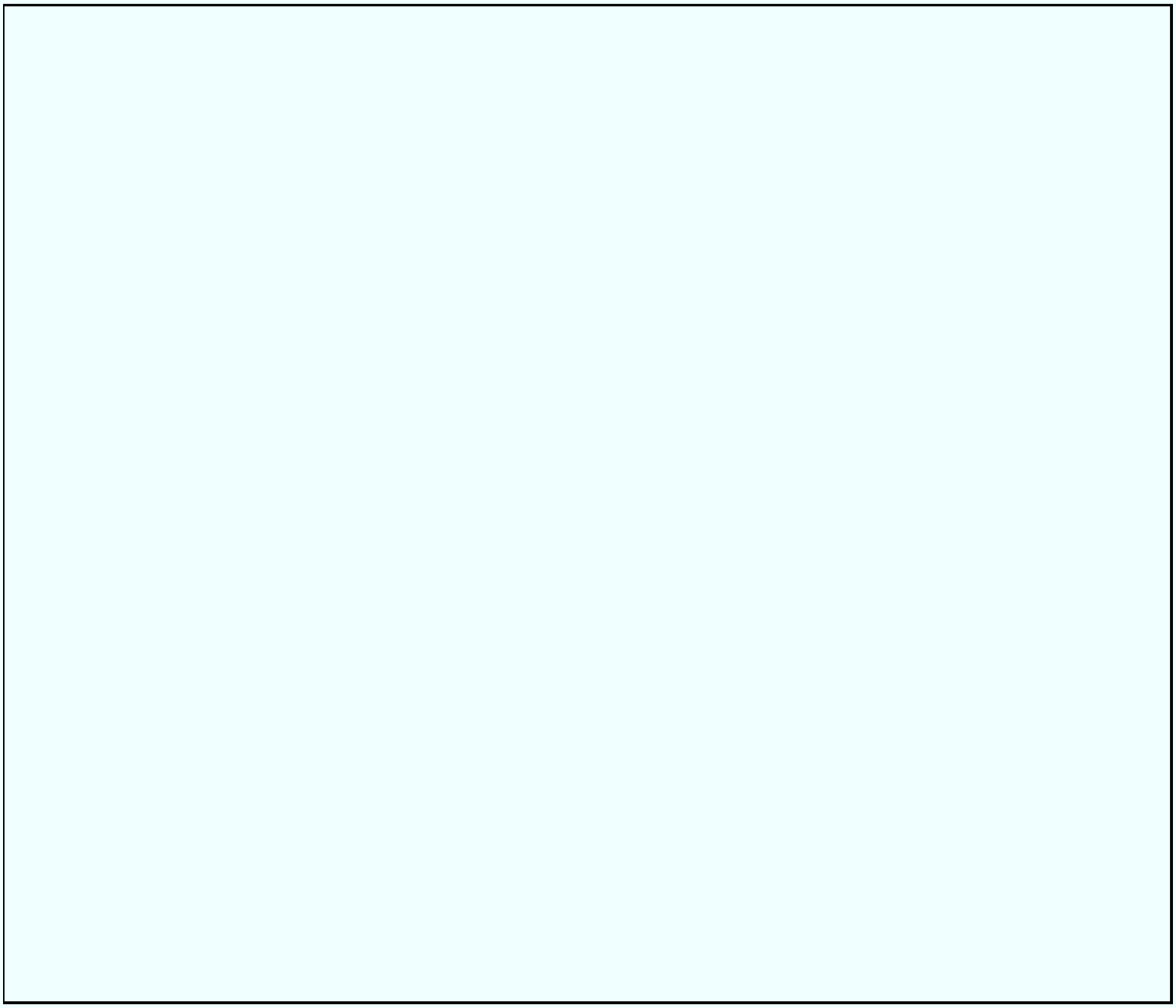
b5
b1

[redacted] (S)

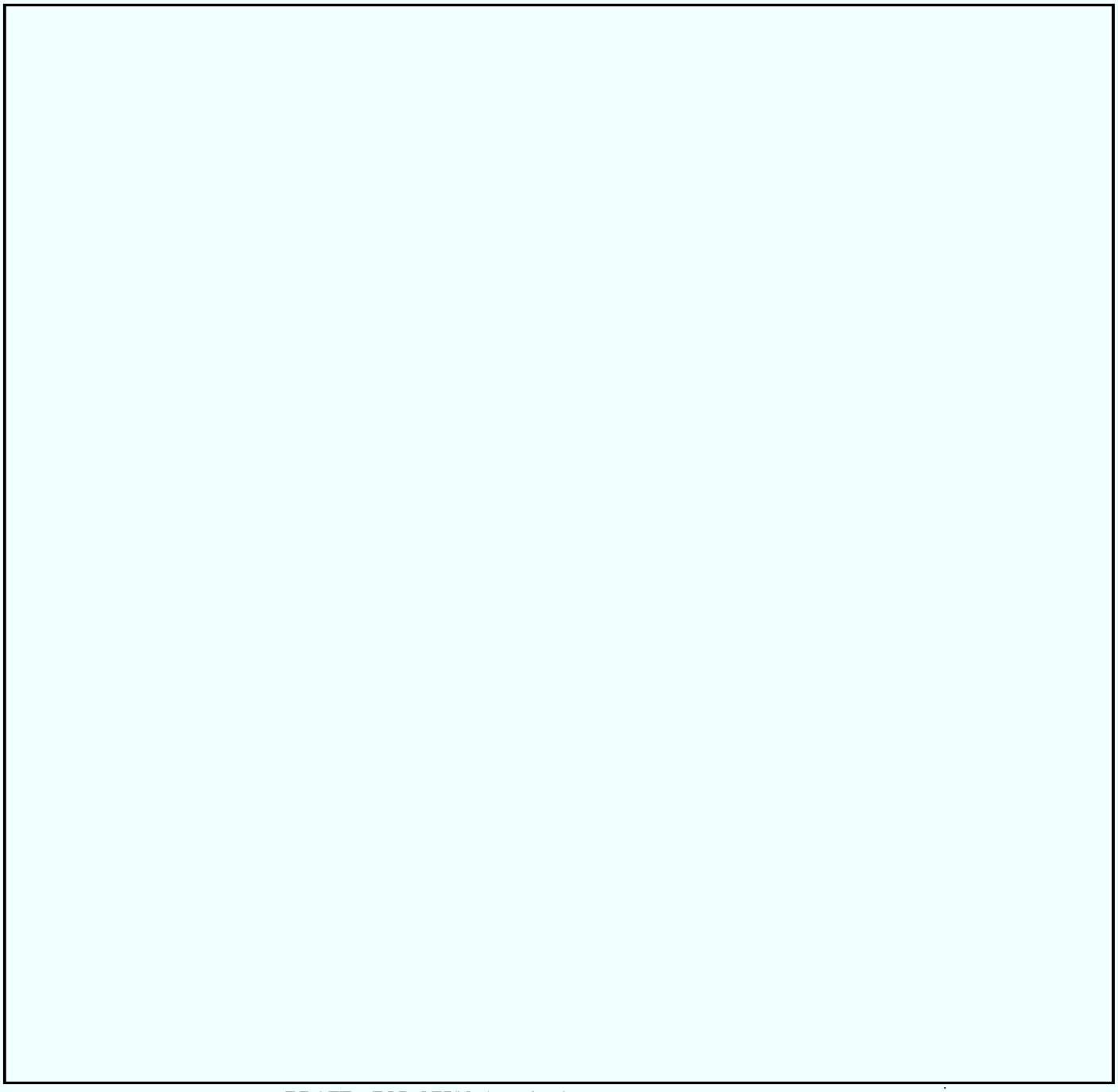
b1
b5

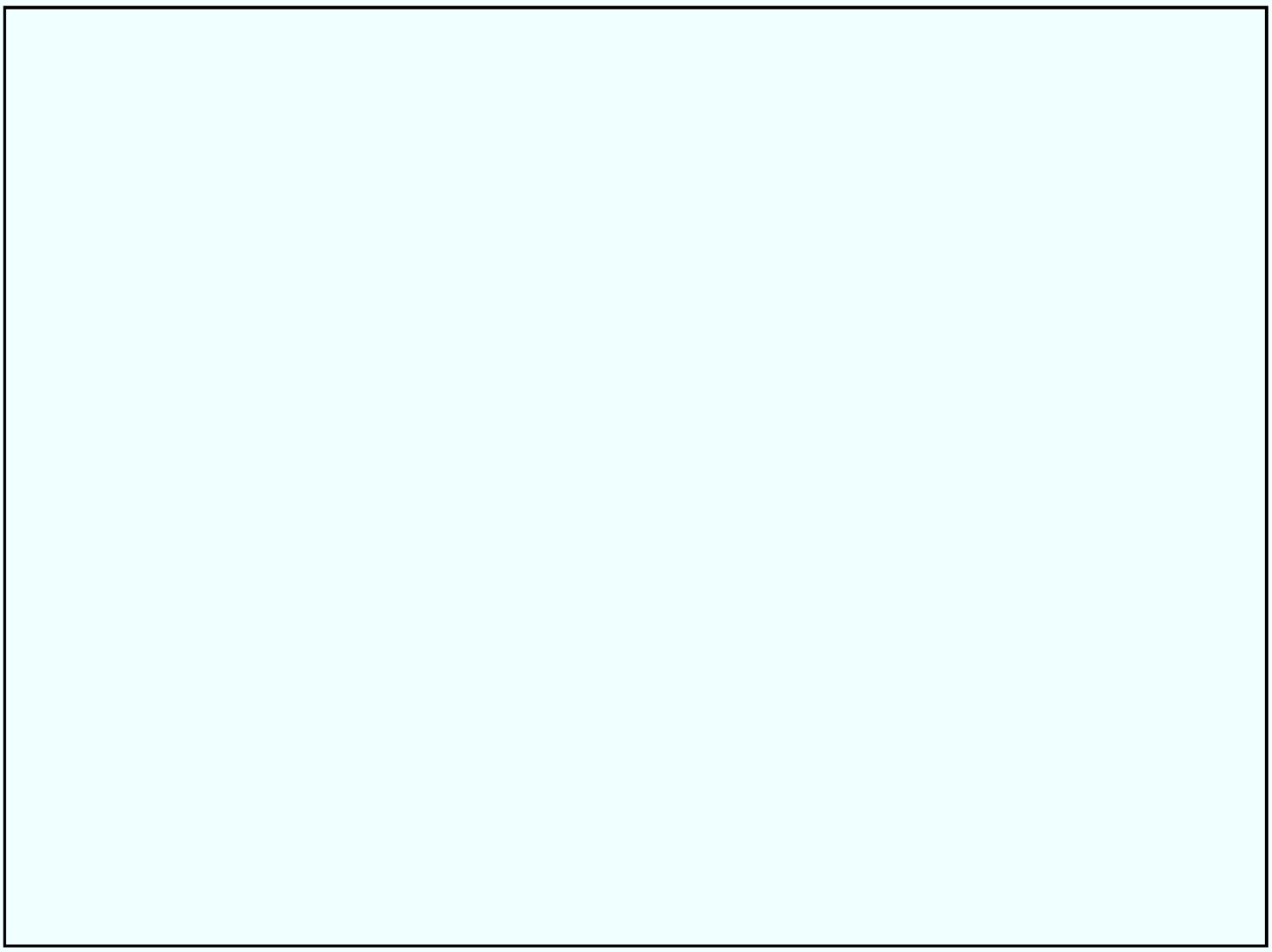
[redacted] b5

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT



b5





ÄÁ□Ø Ø □□ÁTerrorist DNA database

b5
b6
b7C

Đ□Đ□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□°□□□`
□□h□À□□□p□È□ x Đ (#€%Ø'0*^,à.81□3è5@8~:õ<H? AøCPF¨H□KXM°O□R`T V□Yh[À]
□`□□□□□□□□□□□□□□□□□□□□□□□□°□Đ□□[redacted]

[redacted]

[redacted] b5

Á□□□□□
□ÁÁ□□□□□
□ÁÁ□□□□□
□ÁÁ□□□□□
□ÁÁ□□□□□
□Á
Á□□□□ [redacted] b5
□Áa.

Á□□□□□ [redacted]
□Áb.

[redacted]

Á□□□□ [redacted]

[redacted] b5

Á□□□□□ [redacted]
□Á2)

[redacted] b5

Á□□□ [redacted]

[redacted] b5

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5
b6
b7C

Ð□Ð□□□□□□□□Q□□Ø ÿÿ□□□□□□□□□□□□□□□□□□□□□□□□□□□°□Ð□□Ð
Ã

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

ÃCC:Ä

ÄÁ□Ø Ø □ [redacted]

b5
b6
b7C

Information Sharing Requirements

PATRIOT ACT

§ 203 ***Authority to share criminal investigative information***

(a) ***Authority to share grand jury information***

(1) Rule 6(e)(3)(C) of the Federal Rules of Criminal Procedure is amended by the following:

(C)(i) Disclosure of grand jury information may be made-

(V) when matters involve foreign and counter intelligence (as defined in the National Security Act) or foreign intelligence information (as defined in (iv)) to any federal law enforcement, intelligence, protective, immigration, national defense, or national security official.

(iv) "Foreign intelligence" means -

(I) Information, whether or not concerning a United States person, that relates to the ability of the United States to protect against the following actions by a foreign power or agent of a foreign power: (aa) actual or potential attack or grave hostile acts; (bb) sabotage or international terrorism; (cc) clandestine intelligence activities by an intelligence service or network; or

(II) Information, whether or not concerning a United States person, with respect to a foreign power or a foreign territory that relates to (aa) the national defense or security of the United Sates; or (bb) the conduct of the foreign affairs of the United Sates.

(b) ***Authority to share electronic, wire, and oral interception information***

(6) Any law enforcement officer may disclose wire, oral, and electronic information, which includes foreign intelligence or counterintelligence information, to any other federal law enforcement, intelligence, protective, immigration, national defense, or national security official.

(c) ***Procedures***

The AG shall establish procedures for the disclosure of grand jury and electronic, wire, and oral interception information that identifies a United States person as defined in FISA.

(d) ***Foreign Intelligence information***

(1) Notwithstanding any other provision of law, it shall be lawful to disclose information obtained as part of a criminal investigation.

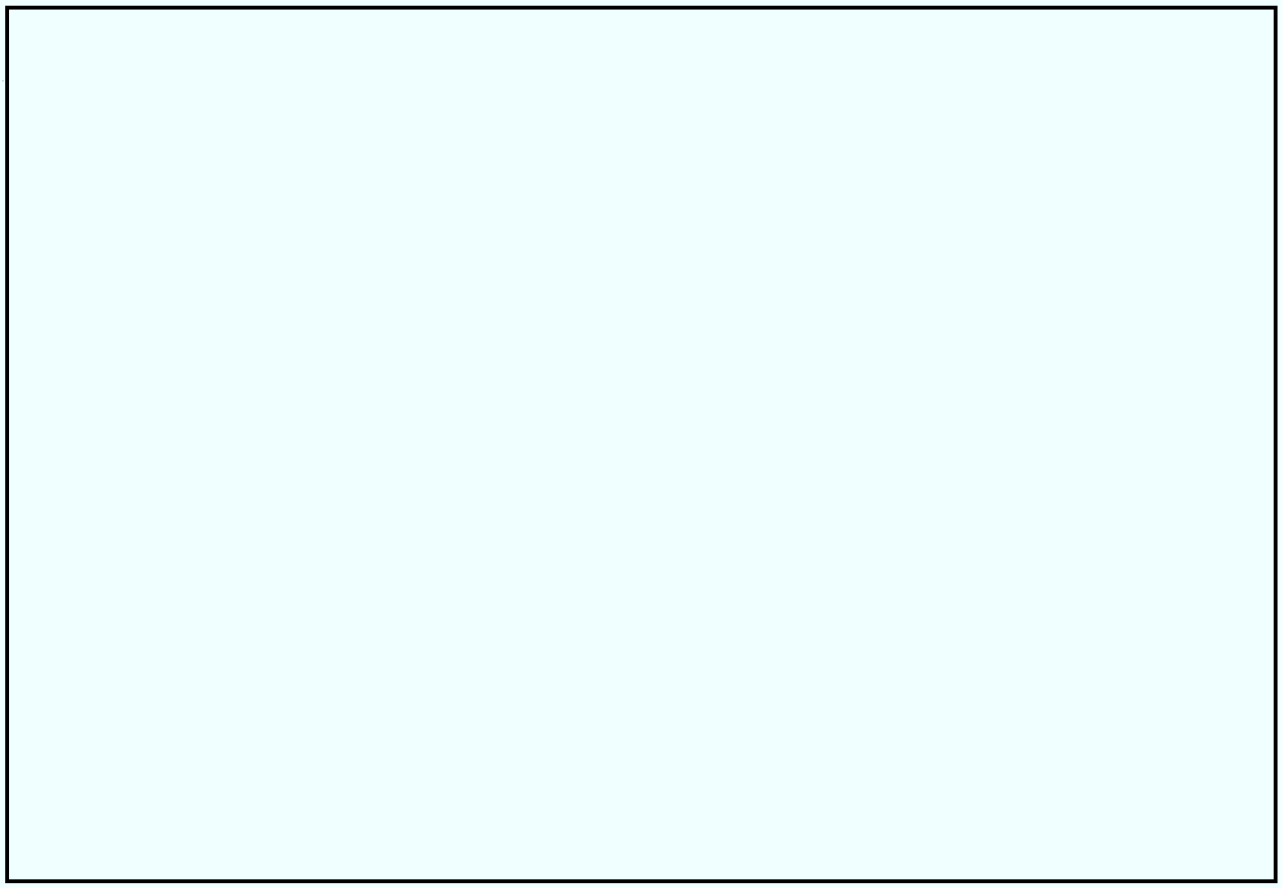
§ 905 ***Disclosure to the DCI of Foreign Intelligence-related information with respect to criminal investigations***

[§ 905 amends Title I of the National Security Act of 1947]

(a) Except as otherwise provided by law, the AG or head of any other department or agency with law enforcement responsibilities shall expeditiously disclose to the DCI foreign intelligence acquired in the course of a criminal investigation pursuant to guidelines developed by the AG and DCI. The AG and the DCI may provide for exceptions if disclosure would jeopardize an ongoing investigation or impair other significant law enforcement issues.

(b) The AG and DCI shall develop guidelines to ensure that after receipt of foreign intelligence activity, the AG provides notice to DCI of any intention to commence or decline to commence a criminal investigation.

(c) The AG shall develop procedures for the administration of this section.



HOMELAND SECURITY ACT
TITLE II – INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION
SUBTITLE A – DIRECTORATE FOR INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION; ACCESS TO INFORMATION
§ 201 ***Directorate for Information Analysis and Infrastructure protection***
(d) ***Responsibilities of the Undersecretary***

The responsibilities of the Undersecretary for Information Analysis and Infrastructure Protection of the Department of Homeland Security ("DHS") shall be as follows:

(4) to ensure, pursuant to section 202, the timely and efficient access by the DHS to all information necessary to discharge the responsibilities under this section, including obtaining such information from other federal agencies.

(9) to disseminate, as appropriate, information analyzed by the DHS to other federal agencies with responsibilities relating to homeland security in order to assist in the deterrence, prevention, preemption of, or response to, terrorist attacks.

(10) to consult with the DC I and other intelligence, law enforcement, or other agencies to establish collection priorities and strategies for information, including law enforcement-related information, relating to threats of terrorism.

(12) to ensure that

(A) any material received pursuant to this Act is protected from unauthorized disclosure.

(B) any intelligence information obtained is shared, retained, and disseminated consistent with the authority of the DCI to protect intelligence sources and methods under the

NSA of 1947 and, as appropriate, similar authorities of the AG concerning sensitive law enforcement information.

(13) to request additional information from federal agencies relating to threats of terrorism, including the entry into cooperative agreements through the Secretary of Homeland Security ("Secretary") to obtain such information.

(17) to coordinate with elements of the intelligence community and with federal, state, and local law enforcement agencies, as appropriate.

§ 202 ***Access to information***

(a) In general –

(1) ***Threat and vulnerability information***

Except as otherwise directed by the President, the Secretary shall have such access as the Secretary considers necessary to all information, that may be collected, possessed, or prepared by a federal agency, relating to threats of terrorism and concerning the infrastructure and vulnerabilities of the United States to terrorism and to other areas of responsibility assigned by the Secretary, whether or not such information has been analyzed.

(2) ***Other information***

The Secretary shall also have access to other information relating to matters under the responsibility of the Secretary that may be collected, possessed, or prepared by a federal agency as the President may further provide.

(b) ***Manner of access***

Except as otherwise directed by the President-

(1) The Secretary may obtain information upon request and may enter into cooperative agreements to provide the information to others or provide the DHS with access to it on a regular or routine basis, including requests or arrangements involving broad categories of material, access to electronic databases; and

(2) Regardless of whether the Secretary has made any request or entered into any cooperative agreement, all federal agencies shall promptly provide the Secretary with the following information:

(A) all reports (include those not yet fully evaluated) relating to threats of terrorism and to other areas of responsibility of the Secretary.

(B) all information concerning the vulnerability of the infrastructure or other vulnerabilities of the United States to terrorism, whether or not such information has been analyzed.

(C) all other information relating to significant and credible threats of terrorism, whether or not such information has been analyzed.

(D) such other information or material as the President may direct.

(c) ***Treatment under certain laws***

The Secretary shall be deemed to be a federal law enforcement, intelligence, protective, national defense, immigration, or national security official, and shall be provided with all the information law enforcement is required to give to the DCI under any provision of the Patriot Act, Section 2517(6) of title 18 USC and Rule 6(e)(3)(C) of the Federal Rules of Criminal Procedure.

(d) ***Access to intelligence and other information***

(1) ***Access by elements of federal government-***

Nothing in this title shall preclude the intelligence community (as defined in the National Security Act of 1947) or any element of the Federal Government with responsibility for

analyzing or receiving any information.

(2) ***Sharing of information***

The Secretary, in consultation with the DCI, shall ensure that intelligence or terrorism-related information to which they have access is appropriately shared with elements of the Federal Government, as appropriate.

SUBTITLE B – CRITICAL INFRASTRUCTURE INFORMATION

§ 212 ***Definitions***

In this subtitle:

(1) "Agency" has the meaning given in 5 USC § 551.

(2) "Covered federal agency" means the DHS.

(3) "Critical Infrastructure Information" means nonpublic information relating to the security of critical infrastructure or protected systems -

(A) Interference with or attack on critical infrastructure or protected systems by either physical or computer-based attack that violates the law, harms interstate commerce, or threatens public health or safety.

(B) The ability of any critical infrastructure or protected system to resist such interference, including any planned or past assessment of the vulnerability of critical infrastructure or a protected system.

(C) Any planned or past operational problem or solution regarding critical infrastructure or protected systems.

(6) "Protected system"

(A) means any service, physical or computer-based system, process or procedure that directly or indirectly affects the viability of a facility or critical infrastructure; and

(B) includes any physical or computer-based system or any component hardware or element thereof, software program, processing instructions, or information or data in transmission or storage therein, irrespective of the medium of transmission or storage.

(7) "Voluntary" -

(A) In the case of submittal of critical infrastructure information to a covered federal agency, "voluntary" means the submittal thereof, without the agency compelling access or submission, that may be accomplished by a single entity or an Information Sharing and Analysis Organization on behalf of itself or its members. ("Information Sharing and Analysis Organization" defined in §212(5)).

(B) Exclusions to the definition of "voluntary" consist of actions brought under the securities laws and do not include information or statements regarding licensing or permitting determinations.

§ 214 ***Protection of voluntary shared critical infrastructure information***

(a) ***Protection***

(1) Notwithstanding any other provision of law, critical infrastructure information that is voluntarily submitted to a covered federal agency for use regarding security of critical infrastructure and protected systems when accompanied by an express statement specified in (2)-

(A) shall be exempt from disclosure under the Freedom of Information Act.

(B) shall not be subject to any agency rules or judicial doctrine regarding ex parte communications with a decision making official.

(D) shall not without written consent of the person or entity submitting such information be used or disclosed by any officer or employee of the United

States for purposes other than those of this subtitle, except: (i) in furtherance of a criminal investigation or prosecution; or (ii) to Congress or the Comptroller General.

(2) ***Express Statement***

"Express statement" means

(A) in the case of written information or records, a written marking indicating that the information is voluntarily submitted in expectation of protection from disclosure.

(B) in the case of oral information, a similar written statement submitted within a reasonable time following the oral communication.

(d) ***Treatment of voluntary submittal of information***

Voluntary submittal of information protected from disclosure by this subtitle shall not be construed to constitute compliance with any requirement to submit such information to a federal agency under any other provision of law.

SUBTITLE C – INFORMATION SECURITY

§ 221 ***Procedures for sharing information***

The Secretary shall establish procedures on the use of information sharing under this title that

(3) protect the constitutional and statutory rights of any individuals who are subjects of such information.

TITLE VIII

SUBTITLE I – INFORMATION SHARING

§ 892 ***Facilitating homeland security information sharing procedures***

(a) ***Procedures for determining extent of sharing of homeland security information***

(1) The President shall prescribe and implement procedures applicable to all federal agencies for sharing homeland security information; identifying and safeguarding sensitive but unclassified homeland security information; and determining whether, how, and to what extent to remove classified information.

(b) ***Procedures for sharing of homeland security information***

(1) Under procedures prescribed by the President, homeland security information shall be shared to the extent such information can be shared and together with assessments of credibility.

(2) Each homeland security information sharing system shall (A) be able to transmit classified and unclassified information; (B) restrict delivery to specific recipients; (C) allow efficient and effective sharing; and (D) be accessible to state and local personnel.

(3) The procedures for sharing homeland security information shall establish conditions (A) to limit redissemination; (B) ensure security and confidentiality; (C) protect constitutional and statutory rights of individuals; and (D) provide data integrity through timely removal and destruction of obsolete and erroneous information.

(5) Each appropriate federal agency, as determined by the President, shall have access to the information described under paragraph (1).

(7) Under procedures developed by the DCI and the AG, each federal agency shall review and assess information gathered and shared by local and state agencies and integrate such information with existing intelligence.

(f) ***Definitions***

(1) "Homeland security information" means any information possessed by an agency that (A)

relates to the threat of terrorist activity; (B) relates to the ability to prevent, interdict, or disrupt terrorist activity; (C) would improve the identification or investigation of a suspected terrorist or terrorist organization; or (D) would improve the response to a terrorist act.

(2) "Intelligence community" has the meaning given in § 401a(4) of the National Security Act of 1947.

§ 896 ***Authority to share electronic, wire, and oral interception information***

Amends 18 USC 2517.

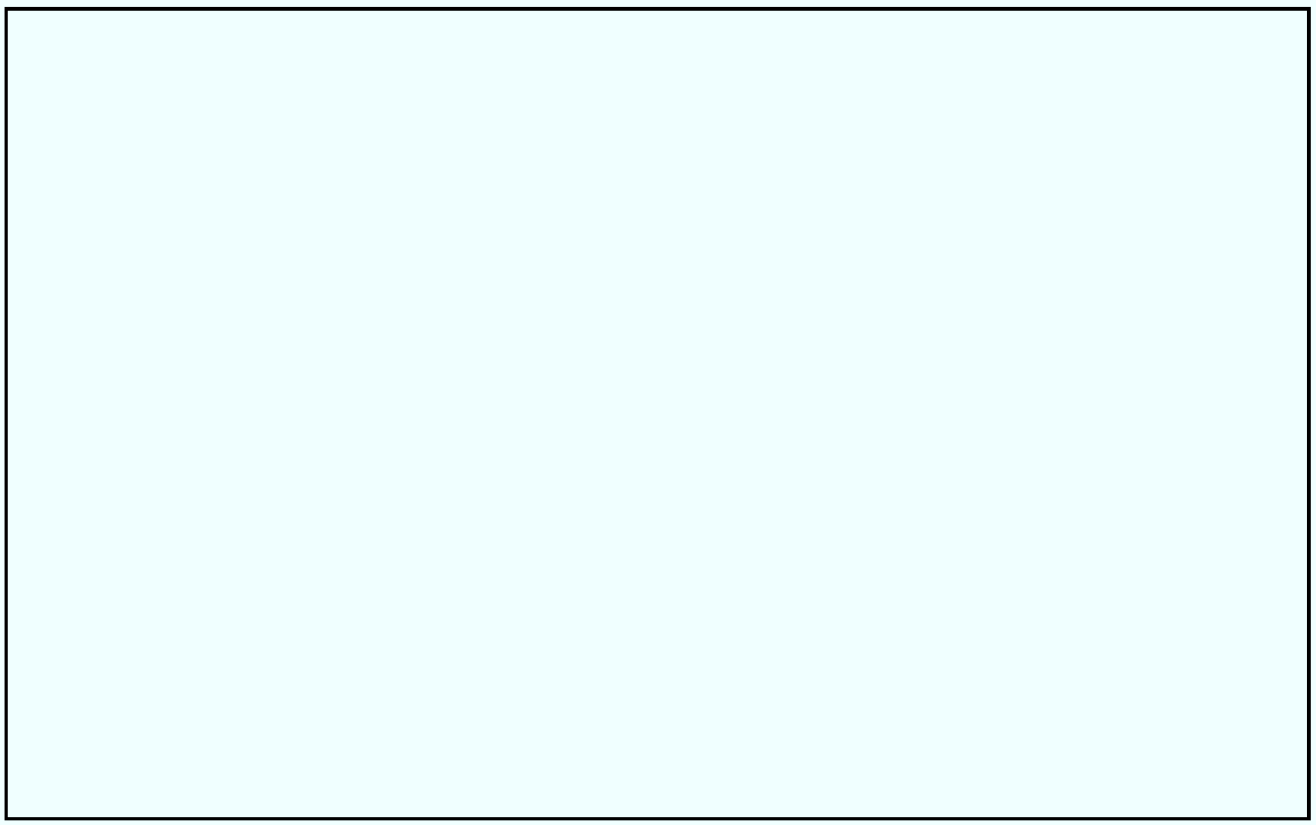
(7) Any investigative or law enforcement officer may disclose wire, oral, or electronic communication or evidence derived therefrom to a foreign investigative or law enforcement officer and vice versa.

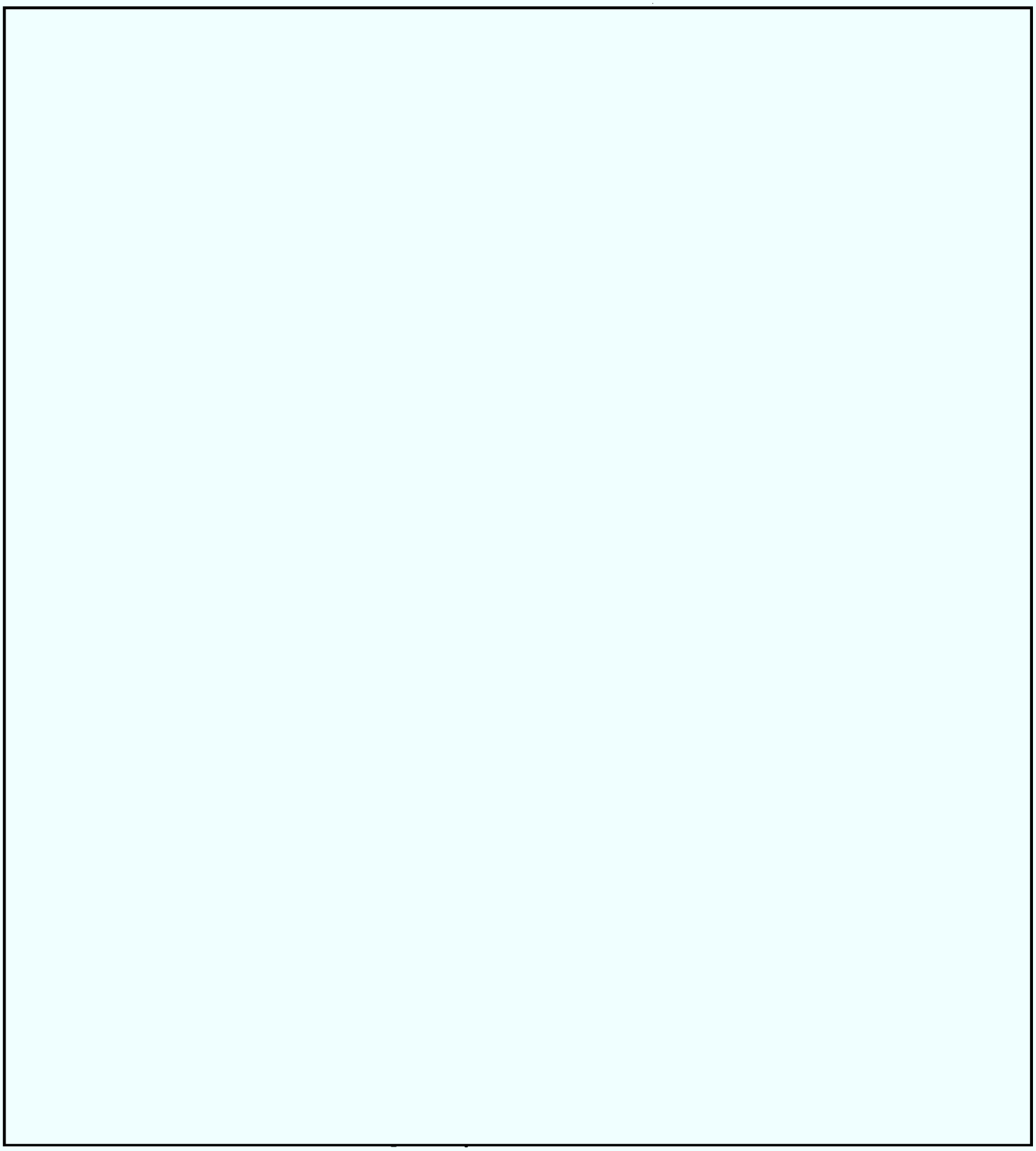
(8) Such information may be disclosed to any federal, state, local, or foreign government official when necessary to prevent or respond to threats of terrorist attacks, hostile acts, sabotage, or clandestine intelligence gathering activities by a foreign power or its agent ("threats of terrorism"). State, local, and foreign governments must follow guidelines issued by the AG and DCI.

§ 897 ***Foreign Intelligence Information***

(a) ***Dissemination authorized***

Amends Patriot Act section 203(d). It shall be lawful to disclose information revealing threats of terrorism obtained as part of a criminal investigation to appropriate federal, state, local, and foreign government officials for the purpose of preventing or responding to such threats. State, local, and foreign governments must follow guidelines issued by the AG and DCI.





NATIONAL SECURITY ACT OF 1947
§ 401a ***Definitions***
(1) "Intelligence" includes foreign intelligence and counterintelligence.

(2) "Foreign intelligence" means information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities.

(3) "Counterintelligence" means information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations, conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities.

(4) "National intelligence" and "intelligence related to the national security"-

A) each refer to intelligence which pertains to the interests of more than one department or agency of the Government; and

(B) do not refer to counterintelligence or law enforcement activities conducted by the FBI except to the extent provided for in procedures agreed to by the DCI and AG, or otherwise as expressly provided for in this title.

[See also §§ 403-5a(c), 403-5d(2)]

§ 402a ***Coordination of counterintelligence activities***

(e) ***Coordination of counterintelligence matters with the FBI***

(1) Except as provided in paragraph (5), the head of each department or agency of the executive branch shall ensure that-

(A) the FBI is advised immediately if classified information is or was disclosed in an unauthorized manner to a foreign power or agent.

(B) the FBI is consulted with respect to all subsequent actions which may be undertaken by the department or agency to determine the source of such loss or compromise, and

(C) Where the FBI undertakes investigative activities, the FBI is given complete and timely access to the department or agency's employees and records.

(2) Except as provided in paragraph (5), The Director of FBI shall ensure that espionage information pertaining to departments or agencies is provided to them in a timely manner and that they are consulted in a timely matter with respect to espionage investigations that concern them.

(3)

(A) The Director of FBI shall submit to the department or agency a written assessment of the potential impact of their actions on counterintelligence investigations.

(B) The department or agency shall evaluate the assessment to determine whether the subject of the investigation should be left in place and notify the FBI of such determination.

(C) The department or agency and the FBI shall continue to consult, review the status of the investigation, and reassess.

(5) When extraordinary circumstances affect national security, the President may on a case-by-case basis waive the requirements above.

§ 403-3 ***Responsibilities of the DCI***

(c) ***Head of the intelligence community***

(6) The DCI shall establish requirements for the collection of FI under FISA and provide assistance to the AG in disseminating information from electronic surveillance and physical searches under FISA. Except as otherwise authorized by statute or executive order, the DCI has no authority to direct, manage, or undertake electronic surveillances or physical searches pursuant to FISA.

(d) ***Head of the CIA***

(3) The DCI shall correlate, evaluate, and provide appropriate dissemination of intelligence related to national security.

§ 403-4 ***Authorities of the DCI***

(a) *Access to intelligence*

The DCI shall have access to all intelligence related to national security that is collected by any department, agency, or other entity of the United States (to the extent recommended by the NSC and the President).

§ 403-5a ***Assistance to United States law enforcement agencies***

(a) ***Authority to provide assistance***

Elements of the intelligence community may, upon request of United States law enforcement agencies, collect information outside the United States about individuals who are not United States persons, notwithstanding the intention of law enforcement agencies to use such information for law enforcement or counterintelligence investigations. (This is subject to limitations imposed by the DoD).

(c) ***Definitions***

(1) "United States law enforcement agency" means any department or agency of the Federal government that the AG designates as a law enforcement agency for the purposes of this section.

(2) "United States Person" means

(A) US citizen

(B) permanent alien resident

(C) unincorporated association composed of citizens or resident aliens

(D) corporation incorporated in the US (except for those directed or controlled by foreign governments).

§ 403-5b ***Disclosure of foreign intelligence acquired in criminal investigations; notice of criminal investigations of foreign intelligence sources***

(a) ***Disclosure of foreign intelligence***

(1) Except as otherwise provided by law, the AG or other law enforcement head shall expeditiously disclose to DCI, pursuant to guidelines developed by AG, FI acquired by the DOJ in the course of a criminal investigation.

(2) The AG can provide for exceptions if the AG determines that disclosure would jeopardize an ongoing law enforcement investigation or impair other significant law enforcement interests.

(b) ***Procedures for notice of criminal investigations***

The AG and DCI will develop guidelines to ensure that, after receipt of a report from the intelligence community about FI warranting a criminal investigation, the AG provides notice to the DCI within a reasonable period of time of any intention to commence or decline to commence a criminal investigation.

(c) *Procedures*

The AG shall develop procedures for the administration of this section.

§ 403-5d ***Foreign Intelligence information***

(1) ***In general***

Notwithstanding any other provision of law, it shall be lawful for FI obtained as part of a criminal investigation to be disclosed to any federal law enforcement, intelligence, protective, immigration, national defense, or national security official.

(2) ***Definitions***

"Foreign intelligence" means

(A) information, whether or not concerning a United States person, that relates to protection against the following actions by a foreign government or its agents: (i) actual or potential attacks or hostile acts; (ii) sabotage or international terrorism; (iii) clandestine intelligence activities.

(B) information, whether or not concerning a United States person, with respect to a foreign power or agent that relates to: (i) national defense or security; (ii) conduct of the foreign affairs of the United States.

EO 12333

Part 1

Goals, Direction, Duties and Responsibilities with respect to the National Intelligence Effort

1.1 ***Goals***

The United States intelligence effort shall provide the President and National Security Council with necessary information on which to base the conduct and development of foreign, defense, and economic policy, and the protection of the United States national interests from foreign security threats. All departments and agencies shall cooperate fully.

(a) Maximum emphasis should focus on analytical competition among the intelligence community.

(b) All means, consistent with United States law and this Order, and with full consideration of the rights of US persons, shall be used to develop intelligence.

(d) To the greatest extent possible consistent with applicable United States law and this Order, and with full consideration of the rights of US persons, all agencies shall ensure full and free exchange of information.

1.4 ***The Intelligence Community***

In accordance with applicable US law and with the other provisions of this Order, agencies within the Intelligence Community shall:

(a) Collect information needed by the President, the National Security Council, the Secretaries and State and Defense, and other Executive Branch officials.

(b) Protect and disseminate intelligence.

(c) Collect information concerning intelligence activities directed against the United States and concerning activities to protect against such conduct.

1.5 ***Director of Central Intelligence***

The DCI shall be responsible directly to the President and the NSC and shall:

(a) Act as their primary advisor on foreign national intelligence and provide them and other officials within the Executive Branch with national foreign intelligence.

(i) Establish uniform criteria for determining relative priorities for the transmission of critical national foreign intelligence.

(k) Have full responsibility for producing and disseminating national foreign intelligence. Have authority to levy analytic tasks on departmental intelligence production organizations, ensuring that competitive analysis, diverse points of view, and differences of judgment are brought to the attention of national policy makers.

(l) Ensure the timely exploitation and dissemination of foreign intelligence including dissemination to appropriate government entities and military commands.

(m) In accordance with the law and relevant procedures approved by the AG under this Order, give departments and agencies access to all intelligence relevant to their national intelligence

needs.

1.6 ***Duties and Responsibilities of the Heads of Executive Branch Departments and Agencies***

(a) In accordance with the law and AG procedures under this Order, the heads of all executive branch departments and agencies shall give the DCI access to all information relevant to the national intelligence needs of the United States.

1.7 ***Senior Officials of the Intelligence Community***

The heads of departments or agencies within the IC shall:

(f) Disseminate intelligence to cooperating foreign governments under arrangements established or agreed to by the DCI.

1.8 ***The Central Intelligence Agency***

As authorized by this Order, the National Security Act of 1947, the CIA Act of 1949, and appropriate directives or other applicable law, the CIA shall:

(a) Collect, produce, and disseminate foreign intelligence and counterintelligence, including information not otherwise obtainable, in coordination with the FBI under procedures of the AG and DCI.

(b) Collect, produce, and disseminate intelligence on foreign aspects of narcotics production and trafficking.

1.14 ***The FBI***

Pursuant to regulations established by the AG, the Director of the FBI shall:

(d) Produce and disseminate foreign intelligence and counterintelligence.

Part 2

Conduct of Intelligence Activities

2.3 ***Collection of Information***

Agencies within the IC are authorized to collect, retain, or disseminate the following information concerning US persons in accordance with procedures developed by the heads of the agencies and approved by the AG:

(a) Information that is publicly available or collected with the consent of the person concerned.

(b) Information constituting foreign intelligence or counterintelligence, including such information concerning corporations or other commercial organizations.

(c) Information obtained in the course of a lawful foreign intelligence, counterintelligence, international narcotics, or international terrorism investigation.

(d) Information needed to protect the safety of any persons or organizations, including those who are targets, victims, or hostages of international terrorist organizations.

(e) Information needed to protect foreign intelligence or counterintelligence sources or methods from unauthorized disclosure.

(f) Information concerning persons who are reasonably believed to be potential sources or contacts for the purpose of determining their suitability or credibility.

(g) Information arising out of a lawful personnel, physical, or communications security investigation.

(h) Information acquired by overhead reconnaissance not directed at specific US persons.

(i) I ncidentally obtained information that may indicate involvement in activities that may violate federal, state, local, or foreign laws.

(j) I nformation necessary for administrative purposes.

Agencies within the IC can disseminate this information to each other.

2.4 ***Collection Techniques***

The IC cannot use the following collection techniques regarding US persons: electronic surveillance, unconsented physical search, mail surveillance, physical surveillance, or monitoring devices unless they are in accordance with procedures established by the head of the agency and approved by the AG. Such procedures shall protect constitutional and other legal rights, use the least intrusive means possible, and limit the use of such information to lawful governmental purposes.

3.4 *Definitions*

(a) "Counterintelligence" means information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or international terrorist activities, but not including personnel, physical, document or communication security programs.

(d) "Foreign intelligence" means information relating to the capabilities, intentions, and activities of foreign powers, organizations or persons, but not including counterintelligence except for information on international terrorist activities.

(e) "Intelligence activities" means all activities that agencies within the IC are authorized to conduct pursuant to this Order.

(f) "US Person" means a United States citizen, an alien known by the intelligence agency concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporation in the United States, except for a corporation directed and controlled by a foreign government or governments.

From [redacted] (OGC) (FBI)
Sent: Friday, October 22, 2004 7:44 PM
To: [redacted] OGC) (FBI); [redacted] (OGC) (FBI)
Cc: [redacted] (OGC) (FBI); [redacted] OGC) (FBI); THOMAS, JULIE F. (OGC) (FBI)
Subject: RE: INTEL POLICY MANUAL

b6
b7C

b5
b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Friday, October 22, 2004 10:15 AM
To: [redacted] (OGC) (FBI)
Cc: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (CTD) (FBI)
Subject: RE: INTEL POLICY MANUAL

b6
b7C

b5
b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]

[redacted]

[redacted]

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Friday, October 22, 2004 9:44 AM
To: [redacted] (OGC) (FBI)
Cc: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (CTD) (FBI)
Subject: RE: INTEL POLICY MANUAL

b6
b7C
b5
b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Thursday, October 21, 2004 12:20 PM
To: [redacted] (OGC) (FBI)
Cc: THOMAS, JULIE F. (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI)
Subject: RE: INTEL POLICY MANUAL

b6
b7C
b5
b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]

b6
b7C

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Tuesday, October 19, 2004 8:21 PM
To: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI)
Cc: THOMAS, JULIE F. (OGC) (FBI)
Subject: INTEL POLICY MANUAL

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

b6
b7C

[redacted]

Attached is what we hope is the final draft of the Intel Policy Manual you previously reviewed. We have taken into account all of your concerns as best we could, with the possible exception of [redacted] question about subjecting disseminations to the White House to the NSIG. Y'all take a closer look at that issue, in particular, and you don't like it, we can discuss it. I intend to make a side-by-side comparion of an AG memo [redacted] gave me last week with the info-sharing provisions of the NSIG. Absent some epiphany, however, this is how we intend to proceed, unless Valerie tells Maureen it's legally objectionable.

b6
b7C

FYI, in addition to concerns y'all raised specifically, [redacted] and I went back thru the whole thing with the *spirit* of your concerns in mind and rewrote some things y'all did not address. We think the result is a much better product than we had before. OI started this project with intent of producing a 70% solution quickly, then supplementing it as time and experience goes by. That didn't happen. As it turns out, however, I think what's attached in better than 70%, due in no small measure to your participation. So, thanks.

I hate to say we're rushed, but we need to report to the DOJ/IG by the end of the week (or maybe early next week) as to the status of this manual, so I need your comments ASAP.

Homer

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 42
Page 5 ~ Duplicate
Page 6 ~ Duplicate
Page 7 ~ Duplicate
Page 8 ~ Duplicate
Page 9 ~ Duplicate
Page 10 ~ Duplicate
Page 11 ~ Duplicate
Page 12 ~ Duplicate
Page 13 ~ Duplicate
Page 14 ~ Duplicate
Page 15 ~ Duplicate
Page 16 ~ Duplicate
Page 17 ~ Duplicate
Page 18 ~ Duplicate
Page 19 ~ Duplicate
Page 21 ~ Referral/Direct
Page 24 ~ Referral/Direct
Page 25 ~ Referral/Direct
Page 31 ~ Referral/Direct
Page 32 ~ Referral/Direct
Page 124 ~ Referral/Direct
Page 125 ~ Referral/Direct
Page 126 ~ Referral/Direct
Page 127 ~ Referral/Direct
Page 139 ~ Duplicate
Page 140 ~ Duplicate
Page 141 ~ Duplicate
Page 142 ~ Duplicate
Page 143 ~ Duplicate
Page 144 ~ Duplicate
Page 145 ~ Duplicate
Page 309 ~ Duplicate
Page 324 ~ Duplicate
Page 325 ~ Duplicate
Page 326 ~ Duplicate
Page 328 ~ Referral/Direct
Page 329 ~ Referral/Direct
Page 335 ~ Referral/Direct
Page 336 ~ Referral/Direct
Page 337 ~ Referral/Direct
Page 338 ~ Referral/Direct
Page 339 ~ Referral/Direct